
This is the **published version** of the article:

García Tallante, Rubén; Sala Cuberta, Albert, dir. La tecnologia Blockchain, eina per a la transformació financera. 2021. 103 pag. (947 Grau en Comptabilitat i Finances)

This version is available at <https://ddd.uab.cat/record/248144>

under the terms of the  license

FACULTAT D'ECONOMIA I EMPRESA

CAMPUS DE SABADELL



Universitat Autònoma de Barcelona

LA TECNOLOGIA *BLOCKCHAIN*,

EINA PER A LA TRANSFORMACIÓ FINANCERA

RUBÉN GARCÍA TALLANTE

GRAU EN COMPTABILITAT I FINANCES

TUTOR: ALBERT SALA CUBERTA

SABADELL, VINT DE MAIG DE L'ANY DOS MIL VINT-I-U

Agraïments

*A l'Albert Sala, per ensenyar-me
el camí d'aquest treball*

*A la meva família, per ensenyar-me
el camí de la vida*

RESUM DEL TREBALL

Blockchain, un anglicisme amb notorietat creixent a l'actual societat que és traduït com a *cadena de blocs*, tres simples paraules que unides generen una nova dimensió de progrés i disrupció tecnològica gràcies a les propietats revolucionàries aportades per aquest sistema de base de dades distribuïda, inalterable i segura. Tot i ser popularitzada per al món de les criptomonedes de la mà del *Bitcoin*, les característiques úniques de la cadena de blocs obren un ventall d'oportunitats molt valuoses per a sectors que no tenen res a veure amb el seu destí inicial.

Davant de la imminent importància d'aquesta tecnologia, al llarg d'aquest treball s'analitzarà detalladament el valor real que pot obtenir-se del seu ús més enllà de la teoria divulgativa, partint des del nucli de l'arquitectura tecnològica de la base de dades distribuïda fins a l'anàlisi de casos reals en sectors heterogenis on la cadena de blocs genera avantatges competitives notòries. Es veurà com una tecnologia teòricament destinada a canviar el futur ja és clarament una disrupció del present.

PARAULES CLAU

Blockchain, Cadena de Blocs, Base de Dades, Tecnologia.

ABSTRACT

Blockchain, a term with growing notoriety in today's society which is able to generate a completely new dimension of progress and technological disruption due to the revolutionary properties provided by this unalterable and secure distributed database system. Although it was popularized jointly the cryptocurrencies industry side by side with *Bitcoin*, the unique characteristics of the *Blockchain* opens up a range of highly valuable opportunities for sectors that have nothing to do with its original destination.

Given the imminent importance of this technology, throughout this work we will be able to analyze in detail the real value that can be obtained from its use beyond the theoretical data, starting from the core of the technological architecture used in the distributed database to the analysis of real cases in heterogeneous sectors where *Blockchain* can cause notorious competitive advantages. It will be shown how a technology theoretically destined to change our future has been converted into a present disruption.

KEYWORDS

Blockchain, Distributed Ledger, Database, Technology.

TAULA DE CONTINGUTS

1. Origen, Naturalesa i Característiques de la Tecnologia <i>Blockchain</i>	5
2. Síntesi de l'Arquitectura Tecnològica	9
3. Anàlisi del Potencial Assolible amb Tecnologia <i>Blockchain</i>	30
3.1. Noves Relacions Contractuals amb els <i>Smart Contracts</i>	30
3.2. <i>DApps</i> per a una Economia Col·laborativa Real	35
3.3. Millora d'Eficiència al Sector Assegurador	38
3.4. Sinèrgies amb la <i>Internet of Things</i>	40
3.5. El Valor de les Dades, Benefici de la Població Mundial amb <i>DeFi</i>	43
3.6. Les Criptomonedes, <i>Blockchain</i> com a Mètode Transaccional	47
3.7. Les Initial Coin Offering com a Mètode de Finançament	55
3.8. Optimització del Sector Públic	59
3.9. Gestió de Dades Modernitzant la Comptabilitat	64
3.10. Digitalització al Sector Financer	66
3.11. Valoració de l'Elevat Cost Energètic	71
3.12. Tipus de Cadenes de Blocs per a cada Finalitat	73
3.13. Traçabilitat Detallada dels Productes	80
3.13.1. Blockchain Contra la COVID	88
3.14. Valor Generat pels dels <i>Non Fungible Tokens</i>	91
4. Conclusions Sobre el Món d'Oportunitats Generades per la <i>Blockchain</i>	97
Referències Bibliogràfiques	100

1. ORIGEN, NATURALES I CARACTERÍSTIQUES DE LA TECNOLOGIA *BLOCKCHAIN*

En un món marcat per l'exponencial creixement de registres transaccionals, degut principalment a l'augment del valor de les dades al desenvolupar eines per enriquir-se de la seva explotació computacional amb l'obtenció d'informes, no és d'estranyar el fet de que contínuament vagin emergent idees de sistemes i arquitectures tecnològiques per a la gestió eficient de la informació recol·lectada.

Al capdavant d'aquests avenços tecnològics disruptius s'hi troba la *Blockchain*, un sistema de base de dades distribuïda en forma de cadena de blocs, capaç de proporcionar unes característiques úniques que seran desenvolupades i analitzades detalladament als propers capítols.

Per conèixer l'origen d'aquesta nova tecnologia cal remuntar-se a l'any 1991, quan el Doctor en física W. Scott Stornetta i el Doctor en ciències computacionals Stuart Haber varen unir els seus coneixements sobre seguretat criptogràfica aplicada a solucions computacionals, obtenint com a resultat un sistema de documents digitals immutables i consegüentment molt difícils de manipular.

Després de més de deu anys sense donar ús pràctic a aquests grans avenços tecnològics, possiblement per ser idees avançades a la seva època on les eines informàtiques encara no presentaven tant poder computacional ni eren d'ús universal, l'enginyer informàtic Hal Finney va desenvolupar una idea originada dins de la seva afició per la criptografia i que es considerarà com un prototip clau per a la creació de les criptomonedes, aconseguint obtenir un sistema de Proves de Treball Reutilitzables, comunament conegut com a *RPoW* pel seu acrònim en anglès, sent pioner en la creació dels cada vegada més comuns *tokens*, traduït literalment com a fitxa, amb una finalitat de substituir dades sensibles per aquest element que no té valor explotable per si mateix, sinó que va lligat a dades de la xarxa a la que pertany i permet ser intercanviat.

Aquests *tokens*, únics i verificables en cada moment a la base de dades distribuïda, presenten un gran ventall d'oportunitats per a empreses com es mostrarà més endavant.

Plenament immersos en la coneguda com a quarta revolució industrial, marcada per les tecnologies aplicades tant a humans com als objectes mitjançant el *Internet of Things*, unida a una època de crisis econòmica amb sospites i desconfiances cap a un sistema financer basat en intermediaris, com entitats bancaries amb greus carències recordant el cas de Lehman Brothers, apareix a l'any 2008 un document sobre un sistema monetari amb protocol de comunicacions utilitzant codi obert i amb un aspecte revolucionari que progressivament canviarà la història, ja que desenvoluparà un sistema capaç d'enfrontar-se directament contra els diners fiat fiduciaris, el document anomenat *White Paper* de la criptomoneda *Bitcoin*, "*A peer-to-peer electronic cash system*", elaborat per Satoshi Nakamoto.

Tot i que al llegir aquest nom la població generalment interpreta un origen asiàtic per a la criptomoneda més popular del món, res més lluny de la realitat al no existir cap document relacionat amb el continent asiàtic durant els primers anys de la criptomoneda. La identitat real de l'inventor del *Bitcoin* és una de les incògnites més misterioses del que portem de l'actual segle XXI, sobretot per tenir una immensa fortuna mai moguda després d'aconseguir-la els primers mesos de la criptomoneda com es fa constar en el registre de *Blockchain*, obtinguda mitjançant les recompenses que corresponen als usuaris dedicats a comprovar i verificar amb protocols descentralitzats les transaccions de cada bloc aportant poder computacional a la base de dades distribuïda, un procés que és conegut com a mineria de criptomonedes detallat al següent l'apartat, dedicat a l'arquitectura tecnològica.

Aquest cúmul d'actius en propietat intactes arribarien a més d'un milió de *Bitcoins*, o més de 40.000 milions d'euros al canvi actual, per part de Satoshi Nakamoto sense saber realment si aquest és el seu nom real o un simple usuari de correu electrònic, donant lloc a innumerables especulacions entre candidats que presenten certa relació cap a la criptomoneda als seus inicis.

Un dels principals candidats és el mencionat Hal Finney, suposadament havent trobat la clau per l'explotació del seu sistema de Proves de Treball Reutilitzables i havent-se demostrat que va ser el *developer* més involucrat als inicis de la criptomoneda, a més a més sent la primera persona en la història en rebre una transacció en *BTC* el dia dotze de gener de l'any 2009, un moviment de 10 *Bitcoins* que llavors suposava un valor molt inferior a l'euro i que actualment s'hauria revaloritzat fins la vora dels quatre-cents mil euros.

Adicionalment, després de l'obtenció dels primers *Bitcoins* mitjançant mineria de dades el tercer dia de l'any 2009, i la creació del *software* una setmana després, Hal Finney va publicar missatges com un de *Running Bitcoin* just al moment dels primers registres, justificant la seva falta d'activitat pel trist diagnòsi d'Esclerosi Lateral Amiotròfica just l'any del llançament, causant la seva defunció fa gairebé deu anys. Si més no, entre les diverses hipòtesis sobre la identitat de Satoshi Nakamoto també s'hi troba l'opció de que realment darrera d'aquest pseudònim hi hagi un equip d'enginyers o fins i tot una empresa, justificant l'excepcionalitat de la creació i desenvolupament de la criptomoneda. Actualment, sembla que aquest seguirà sent un misteri per a la societat.

Independentment de la identitat dels pioners, varen aconseguir la creació d'un sistema monetari amb criteris notables de desintermediació i descentralització, sense perdre el component de seguretat i inviolabilitat essencial al tractar-se de béns econòmics.

Juntament amb l'arquitectura *peer-to-peer* en una xarxa d'ordinadors que actuen com a nodes que serà analitzada detalladament a l'apartat posterior, comportant-se jeràrquicament igual entre ells sense clients ni servidors fixes, varen aconseguir unir un conjunt de sistemes desenvolupats per altres investigadors a favor de la creació d'una criptomoneda amb fórmula demostradament exitosa pel seu creixement exponencial, sent actualment el *Bitcoin* l'estendard de les criptomonedes.

Seguint l'èxit aconseguit per la moneda electrònica precursora, els darrers anys segueixen apareixent i desenvolupant-se projectes molt interessants per a un gran ventall de sectors, tant empresarials com públics, com és el cas d'una plataforma amb base de dades distribuïda més moderna però també basada en *Blockchain*, creada pel programador rus Vitalik Buterin, i anomenada *Ethereum*.

Aquesta es diferencia del *Bitcoin* i altres criptomonedes gràcies a que l'arquitectura del sistema permet la creació d'aplicacions dins de la pròpia cadena de blocs anomenades *DApps*, i sobretot permet disposar dels emergents *Smart Contracts*, com bé indica el seu nom sent considerats contractes intel·ligents al executar-se dins dels blocs de la *Blockchain* quan es compleixen requisits establerts prèviament, adquirint ambdós les propietats mencionades anteriorment, com la descentralització que proporciona aquest sistema amb creixement exponencial sense la necessitat d'acatar les condicions del sistema financer tradicional, una tecnologia la qual serà minuciosament detallada al següent capítol d'aquest treball.

2. SÍNTESI DE L'ARQUITECTURA TECNOLÒGICA

Paraules com *hash* o *ledger* són termes habitualment desconeguts pel gruix de la societat, les quals seran analitzades detalladament en aquest apartat degut a la importància de conèixer els fonaments tècnics darrera dels sistemes que estan destinats a ser el futur de la nostra societat, al ser la base de l'arquitectura tecnològica que permet generar valor pels usuaris sense que els mateixos perdin la confiança. Si més no, per entendre la naturalesa i funcionament de la *Blockchain* cal anar a l'origen de l'arquitectura tecnològica que permet totes aquestes innovacions.

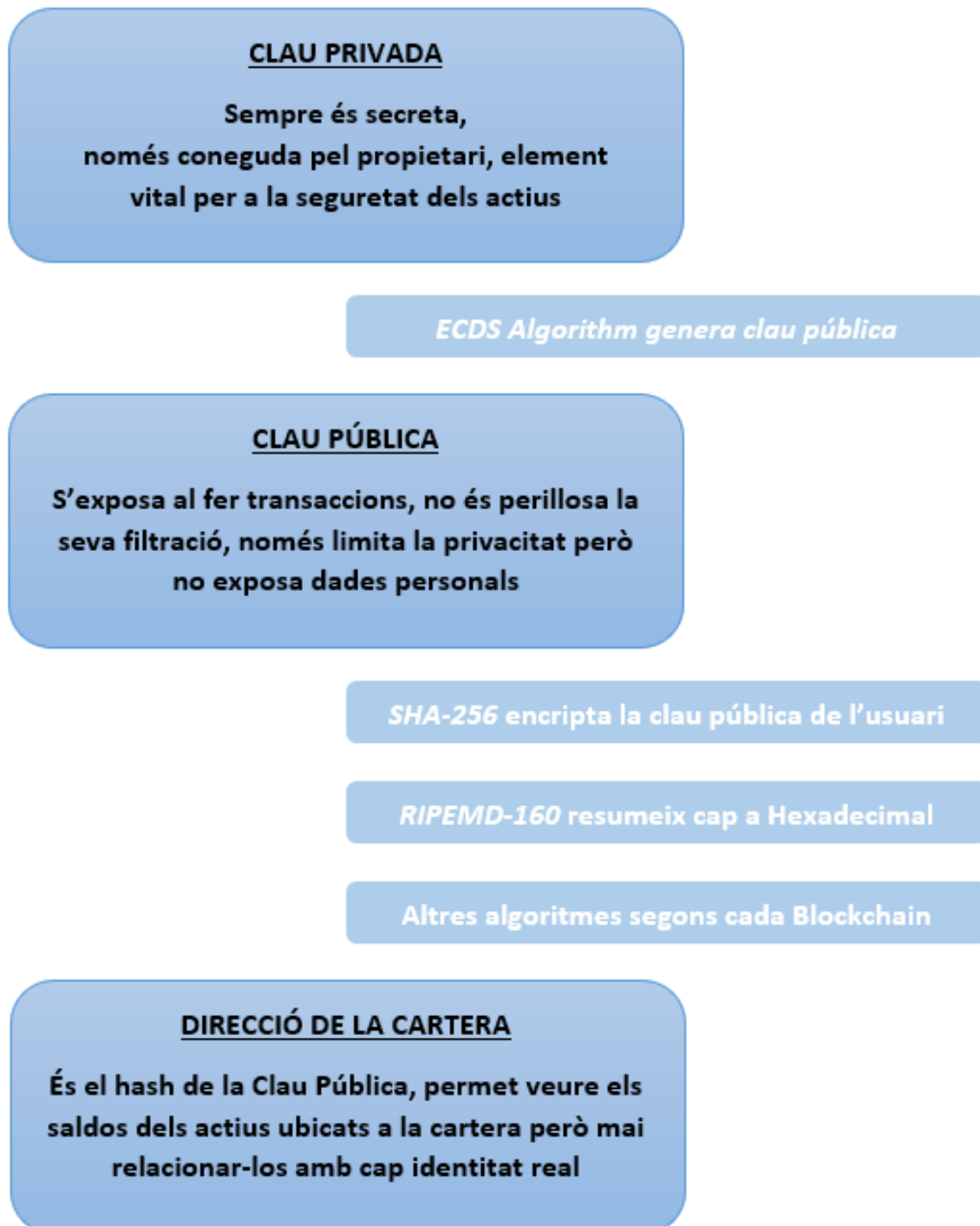
La recurrent paraula criptomoneda, més enllà del aspecte monetari, està formada pel terme cripto, provinent de la criptografia, ja que aquest conjunt de protocols informàtics fa ús d'algoritmes d'enciptació que mitjançant un procediment de xifrat atorguen el suport tècnic necessari per al correcte funcionament de l'ecosistema de les cadenes de blocs que s'utilitza com a base de dades.

Tot i que inicialment varen ser utilitzades cadenes de blocs simples, a l'any 1992 aquestes serien millorades amb la incorporació dels *Merkle Hash Trees* que havia patentat un dels pioners criptogràfics, Ralph Merkle, quan a l'any 1979 va dissenyar una estructura en forma d'arbre dins del propi sistema, encarregant-se de relacionar cadascuna de les transaccions registrades, permetent lligar un gran nombre de les dades incorporades a la base mitjançant una combinació alfanumèrica anomenada *hash*, traduïda literalment com a trossejat, ja que permet obtenir una nova sèrie alfanumèrica de llargada concreta establerta segons la funció matemàtica aplicada a les dades enciptades en cada transacció.

Aquesta funció matemàtica genera un *hash* únic quan és aplicada estrictament al contingut que cal encriptar, provocant consegüentment que en quant canvia mínimament el contingut a encriptar també varia la totalitat del *hash* producte del càlcul matemàtic, saltant la senyal d'alarma per causa de la modificació i aconseguint un nou filtre de verificació sobre la integritat de la informació inclosa a la base de dades distribuïda per molt extensa que sigui la seva grandària, habilitant reunir més d'un document en cada bloc disponible. Gràcies a aquest protocol de *hash*, la inalterabilitat de les dades està plenament garantida, un aspecte notablement disruptiu per a la societat.

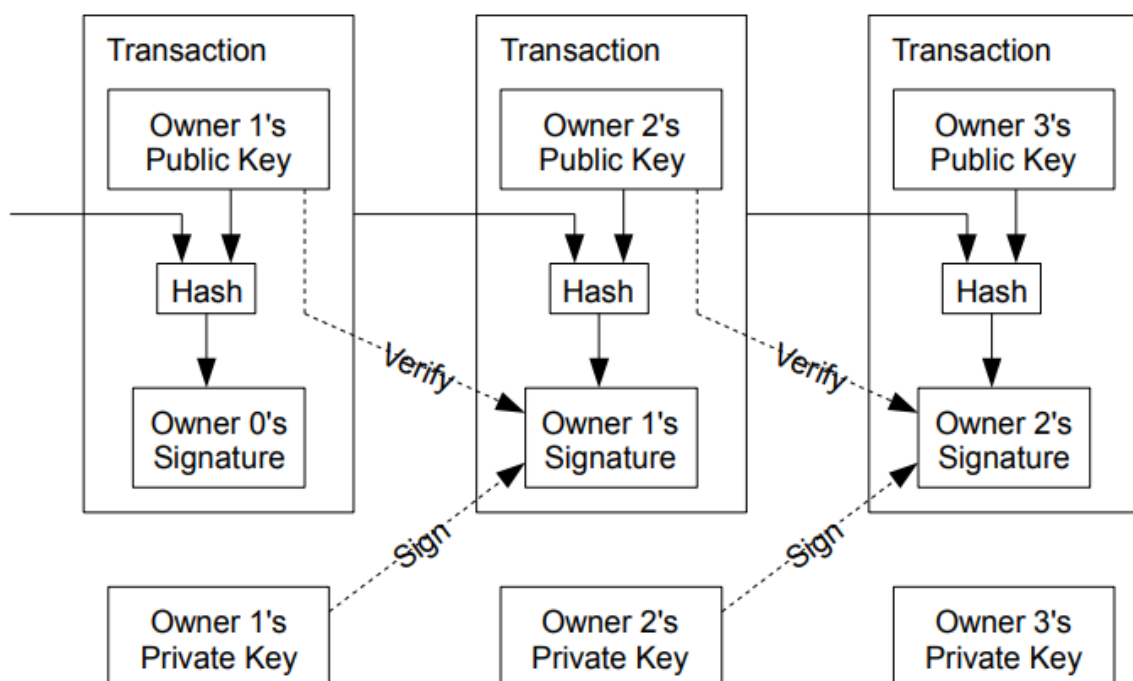
Per als aspectes transaccionals s'ha consolidat com a millor opció criptogràfica la de característiques asimètriques, on els sistemes de criptografia generen una direcció en forma de clau pública habitualment mitjançant l'algoritme anomenat *Elliptic Curve Digital Signature Algorithm* i una altra clau privada completament aleatòria per a cada una de les carteres, amb relació entre ambdues claus. Com és necessari, en cap cas seria viable obtenir la clau privada a partir de la clau pública, pel que és completament segur compartir la clau pública més enllà de que les quantitats econòmiques de les transaccions podrien ser observades per tercers. Aquesta clau de caràcter públic serà la clau encarregada de xifrar els missatges rebuts cap a la seva direcció, podent desxifrar el seu contingut únicament amb la clau secreta de caràcter privat, presentada habitualment en format hexadecimal de setze caràcters alfanumèrics tot i que originalment compten amb una llargada de dos-cents cinquanta sis dígitos en format binari, un format per a reduir les probabilitats de patir un atac informàtic on es provin claus privades aleatòries, sent un escenari amb probabilitat d'ocurrència que tendeix a zero segons els estudis duts a terme, amb ínfimes probabilitats de que això succeeixi i es posi en perill la integritat de les carteres.

Aquesta informació és exposada de manera gràfica a la següent taula d'elaboració pròpia, per a una millor assimilació d'aquest aspecte amb un elevat component de dificultat tècnica.



Il·lustració 1. Elaboració Pròpia. 2021. Esquema de Claus Blockchain

Amb el mencionat binomi de claus codificades, encriptant inicialment amb una clau pública que no podrà ser ella mateixa l'encarregada de desxifrar el contingut de la transacció, afegint seguretat al protocol ja que només el podrà descriptar la clau privada, permet que ningú sense aquesta clau privada pugui fer transaccions però alhora permetent mantenir visible per a tothom la clau pública com a element que actua de manera similar al numero de compte bancari, addicionant-se amb la clau privada que és la que permet únicament al propietari de la cartera fer les transaccions desitjades.



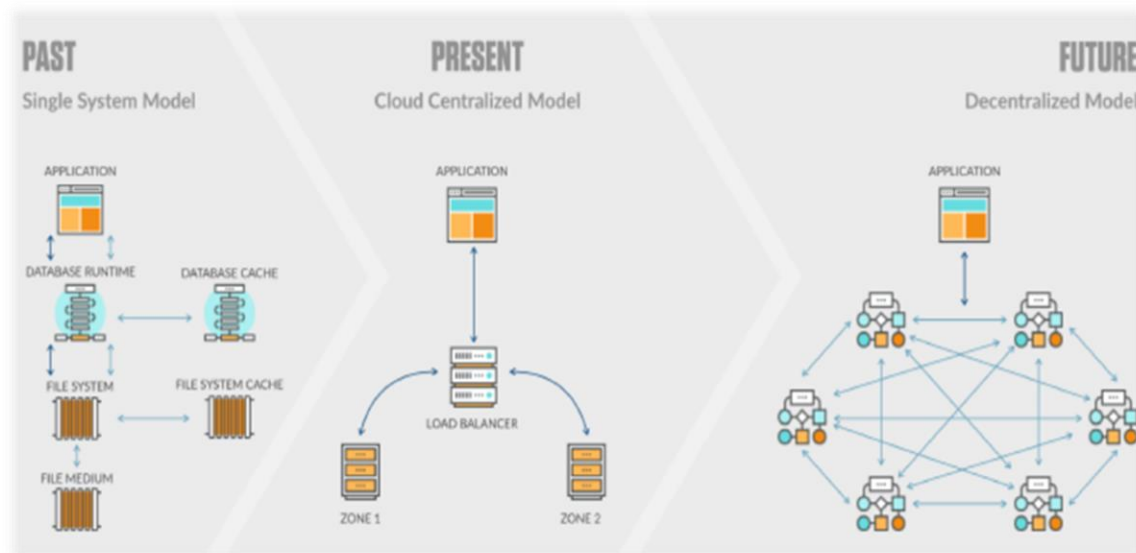
Il·lustració 2. Nakamoto, Satoshi. 2008. Estructura al Bitcoin White Paper. Obtinguda de <https://Bitcoin.org/>

Aquesta encriptació unidireccional també presenta desavantatges en comparació amb els sistemes transaccionals establerts a la societat, ja que operant a través de la cadena de blocs és impossible desfer transaccions, una característica que pot semblar molt beneficiosa en certs escenaris però preocupant per a usuaris que s'equivoquin al introduir la clau pública on volen destinar els seus fons econòmics encara que variï únicament un dígit, ja que alteraria tot el resultat de l'algoritme d'encriptació.

Aquesta característica d'intolerància a l'error és un dels principals hàndicaps de la implementació de les transferències monetàries entre comptes, on un petit error faria perdre tots els fons, entre molts altres casos on els errors humans comportaran pèrdues irreversibles.

Per tant, aquest conjunt estructural dona un component de fiabilitat i eficiència a les xarxes *peer-to-peer*, absolutament necessari per garantir seguretat i transparència sense afectar a la privacitat entre els propis usuaris, adquirint una notablement valuosa capacitat per a certificar i validar dades de qualsevol naturalesa, sense la necessitat d'intermediaris imparcials dins del propi procés transaccional.

Això suposa un immens avenç al comparar-ho amb les xarxes tradicionalment utilitzades, on el component necessari de l'intermediari crea ineficiències transaccionals tant a nivell econòmic i temporal com a nivell de desconfiança, pel possible ús fraudulent del poder d'intermediació.



Il·lustració 3. Kotas, Brett. 2017. Diferències entre Bases de Dades. Obtinguda de www.influencive.com/

Aquest sistema permet conèixer públicament totes les transaccions històriques de la xarxa, habilitant un procediment sense duplicitats i amb una potent verificació entre múltiples nodes beneficiosa per als usuaris, únicament afectant a la seguretat de la cadena de blocs en casos on més de la meitat dels nodes estableixin un consens entre ells, un escenari amb probabilitats ínfimes dins de les cadenes de blocs ja consolidades.

Els mencionats nodes de la xarxa, conjuntament, són els encarregats d'emmagatzemar la pròpia cadena de blocs, evitant així ser guardada a un servidor corruptible, aportant una altra fortalesa a la seva seguretat estructural. Concretament, al tractar-se de xarxes distribuïdes on cada node compta amb una còpia original de la cadena de blocs per a contrastar cadascuna de les modificacions, per alterar el contingut d'una cadena com la del *Bitcoin* caldria un atac simultani que penetri de manera efectiva en la majoria de nodes, un acte catalogable com a impossible degut a l'enorme quantitat de nodes participants a la xarxa d'aquesta tecnologia *Blockchain*.

La mencionada descentralització de la xarxa és un aspecte molt favorable per a la ciberseguretat de la informació, ja que desapareix un únic punt vulnerable a favor tenir les dades distribuïdes per la xarxa, dificultant els atacs per virus informàtics que solen concentrar-se en un únic node o equip informàtic vulnerable. A més a més, un punt molt interessant és que els nodes no queden com a simples receptors d'informació, sinó que poden sol·licitar unir noves dades transaccionals a la xarxa sempre que existeixin altres usuaris que prenguin participació activa a la creació de nous blocs a la cadena, augmentant la capacitat d'emmagatzemar noves dades. A aquest procediment de creació de blocs se l'anomena mineria, sent alguns usuaris voluntàriament miners i encarregant-se de verificar la legitimitat de l'operació per a donar-li validesa si la considera correcta, mitjançant un complex procediment descrit a continuació amb la finalitat d'obtenir una recompensa econòmica a canvi de la creació dels nous blocs.

Aquesta creació de blocs principalment es duu a terme mitjançant dos protocols completament diferents entre si, alternatius, però ambdós estesos entre les *Blockchains* més populars i aconseguint el consens entre els nodes de cadascuna de les xarxes de dades distribuïdes, evitant la duplicitat de transaccions al tractar-se d'un ambient descentralitzat consensuant el registre en ordre d'aparició. El primer d'aquests protocols, utilitzat a grans criptomonedes com el *Bitcoin*, és el conegut com a *Proof of Work*, dut a terme mitjançant la resolució de problemes matemàtics amb dificultat creixent, tot i que el procediment va molt més enllà del simple poder computacional, apareixent la figura dels coneguts com a miners.

Al *PoW*, el procediment de creació de blocs es basa en una incògnita matemàtica la solució de la qual serà fàcilment verificable per tots els nodes de la xarxa, però la seva resolució serà amb un elevat i creixent component de dificultat pel que es requerirà de molt poder computacional, aportat mitjançant equips informàtics principalment dedicats a la mineria com targetes gràfiques o processadors juntament amb l'electricitat necessària per al seu funcionament intens i continuat al llarg del temps. Amb aquests equips informàtics, cadascun dels miners s'encarrega de recopilar les transaccions que encara no han sigut processades cap a ningun bloc de la xarxa, i utilitzen una funció criptogràfica amb diferents combinacions de dades entrants per a obtenir el *hash* del nou bloc de la cadena, dissenyada per l'Agència de Seguretat Nacional dels Estats Units d'Amèrica, anomenada *Secure Hash Algorithm* i coneguda com a *SHA-256*.

Per a una major seguretat i integritat, aquest procediment d'encriptació es duu a terme en dues ocasions, redundant les dades xifrades al obtenir el *hash* definitiu com a producte d'aplicar l'algoritme *SHA-256* sobre el primer *hash* obtingut anteriorment pel mateix algoritme, duplicant la seguretat criptogràfica.

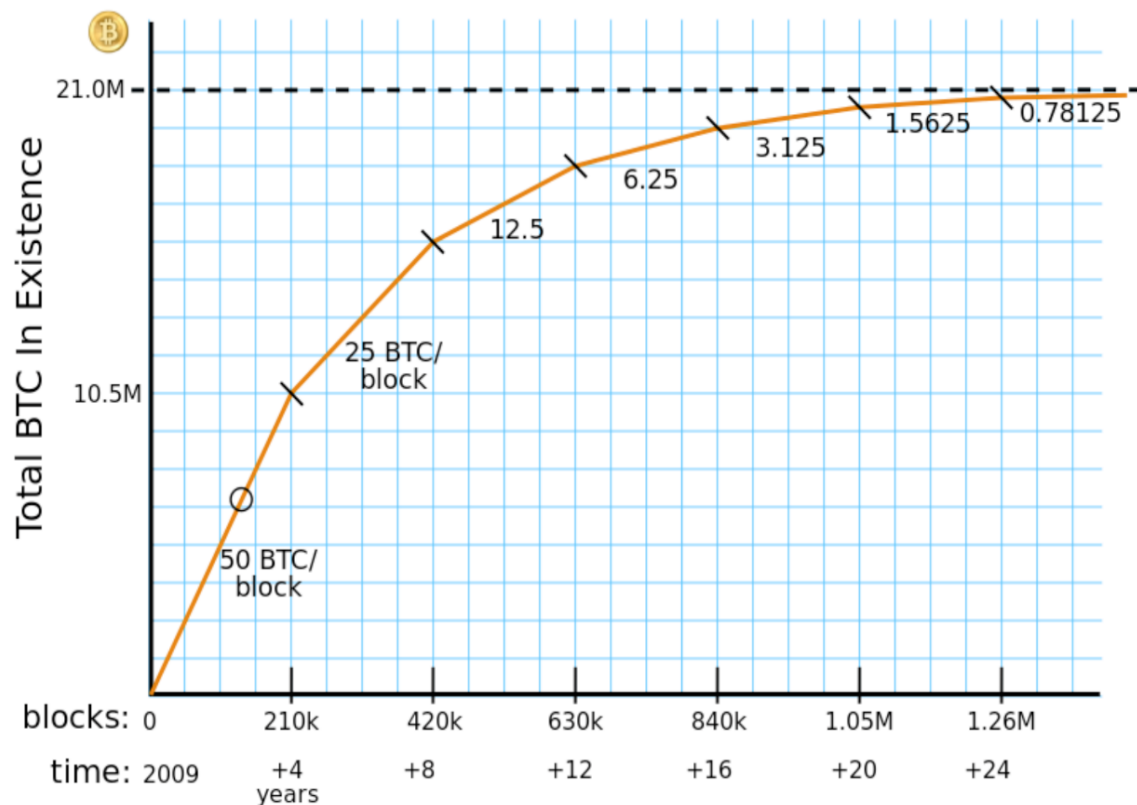
A més a més, amb algoritmes com el *RIPEMD-160* s'aconsegueix ocultar el doble *hash* obtingut del procediment anterior reduint la seva mida per a una major lleugeresa en el processament, filant encara més prim cap a l'excel·lent seguretat que presenten avui en dia aquests procediments.

Tot i així, la immensa majoria de *hash* que obtenen no resulten ser la solució correcta, amb un ritme de prova de respostes conegut com a *hash rate* de 200 quintilions de *hash* per segon a data del 2021, una quantitat d'encert tant reduïda ja que el valor d'aquest *hash* haurà de ser inferior a una quantia actualitzada cada 2.016 blocs i marcada per la situació del mercat en cada moment, adaptant-se a la quantitat de transaccions pendents, actuant favorablement per al correcte funcionament de la cadena de blocs.

La principal premissa establerta comunitàriament és respecte la recompensa atorgada a l'usuari capaç de crear el nou bloc, ja que com la seva aportació a la cadena de blocs és essencial per al correcte funcionament de la mateixa, se'l recompensa amb una quantitat establerta de criptomoneda. Inicialment, la recompensa per bloc creat a la cadena de *Bitcoin* era de cinquanta unitats de *BTC*, valorades en data del 2021 en gairebé dos milions i mig d'euros. No obstant, per a no crear una moneda inflacionària es va establir un límit de vint-i-un milions de *Bitcoin* en circulació, i per a una correcta periodificació de les recompenses Satoshi Nakamoto va dissenyar un model de retribució protagonitzat pels anomenats com a *halvings*.

Aquest terme que traduït literalment significa dividir entre dos, es caracteritza per reduir la mencionada recompensa a la meitat cada 210.000 blocs creats, donant lloc a un sistema deflacionista que augmenta el valor de la moneda a llarg termini ja que permet limitar la oferta disponible encara que creixi la demanda. Per aquesta raó, actualment la recompensa per la creació de cada bloc de la cadena de *Bitcoin* es redueixi dels 50 *Bitcoin* inicials als 6,25 actuals, per un valor actualment proper als tres-cents mil euros.

Tenint en compte que aproximadament cada deu minuts sorgeix la creació d'un nou bloc, és lògic el creixent interès de grans inversions en centres dedicats únicament a la mineria en països que recullin les condicions òptimes, com és una baixa temperatura per als equips informàtics i un cost d'energia elèctrica reduït.



Il·lustració 4. Revista New Money. 2018. BTC en Circulació. Obtinguda de <https://newmoneyreview.com/>

Degut a la gran capacitat computacional necessària per a la mineria d'un bloc sencer, varen sorgir els coneguts com a *mining pools*, els quals compten amb una estructura organitzativa en forma de cooperativa que permet la mineria a qualsevol usuari que compti amb un equip per al procés d'informació com són els ordinadors personals, tot i que òbviament, la recompensa obtinguda per la mineria serà posteriorment repartida equitativament segons el poder de computació aportat per cadascun dels usuaris.

Sempre caldrà que el preu elèctric sigui inferior a la recompensa obtinguda per la creació del bloc ja que sinó no seria rentable dur a terme la mineria, com passa actualment a països com Espanya. Un detall curiós és que l'últim *halving* està programat amb una recompensa de tan sols 0,021 *Bitcoin* per bloc, uns cent euros valorats a l'any 2021, pel que el cost de l'electricitat necessària per al procediment seria clarament superior al benefici obtingut mitjançant la recompensa de validació. Per tant, és molt probable que el *Bitcoin* mai arribi al seu màxim de 21 milions d'unitats emeses, a causa del decreixent atractiu cap a les recompenses de la mencionada mineria.

Aquest sistema també compta amb un important component de seguretat, ja que si com als inicis es tracten d'actius sense valor, difícilment seran atacats i no quedarien escassos els pocs nodes que hi havia a la xarxa abans, als voltants de l'any 2009. D'altra banda, a l'escenari actual on la capitalització de mercat de criptomonedes com el *Bitcoin* és molt elevada, es genera molta atracció cap a delinqüents que intenten corrompre el sistema a favor del seu lucre, però com les recompenses per mineria són de la mateixa manera més atractives, el nombre de nodes treballant pel consens i protecció de la xarxa augmenta significativament. Per tant, és un sistema dinàmic que s'adapta a les condicions de l'escenari en el que es trobi, un aspecte contínuament canviant amb valor molt positiu per a la seguretat.

Davant de noves amenaces per la seguretat de les cadenes de blocs com és la computació quàntica, amb nivells de càlcul mai vistos anteriorment, existeix la possibilitat de dur a terme canvis al protocol de la cadena de blocs que el facin incompatible amb versions anteriors, anomenats com a *hard forks*, pel que caldrà mantenir cert component d'innovació anivellant el grau de seguretat amb les possibles amenaces de delinqüència contra les cadenes de blocs.

Empreses de seguretat tradicional, com Prosegur, estan entrant al mercat de la custòdia d'actius digitals per a institucions mitjançant Prosegur Crypto, el símil virtual del tradicional Prosegur Cash, amb el que aprofiten tant la capacitat protectora física per a carteres fredes de les institucions amb protocols on tenen amplia experiència com gestions segures, i pretenen innovar mitjançant assegurances de les carteres d'actius digitals, aportant confiança i seguretat.

Alternativament al mencionat *Proof of Work* on els propietaris són aquells qui tenen la capacitat de processar les transaccions, es troba el protocol conegut com a *Proof of Stake*, consensuat pels mateixos propietaris de la criptomoneda, convertint-se en el principal estàndard del qual presumeix la segona major criptomoneda al planificar adaptar-lo durant la seva actualització a l'any 2022, l'anomenat *Ethereum 2.0 Serenity*.

Aquest modern procediment de consens per a la creació de blocs és tan prometedor principalment per una característica molt diferenciadora respecte a la alternativa anteriorment detallada, ja que és capaç de validar el consens entre els nodes d'una cadena de blocs mitjançant una selecció ponderada de nodes basada en criteris com la quantitat de criptomonedes en possessió o la antiguitat a la xarxa, entre d'altres.

Una vegada seleccionats els nodes, sempre mantenint una quantitat notable que no suposi cap problema per a la seguretat de la xarxa, aquests validadors podran crear nous blocs obtenint les degudes recompenses. Cal destacar que amb aquest protocol de consens es redueix notablement l'ús energètic al no necessitar el poder computacional per a resoldre els problemes matemàtics del *Proof of Work*, basant el consens en la validació per part de certs propietaris de la xarxa, buscant un objectiu comú que sigui beneficis per a les seves inversions.

Cal mencionar que actualment es pot trobar una gran diversitat de protocols per al consens de les cadenes de blocs, però la gran majoria de *Blockchains* s'acullen a algun dels anteriorment detallats, per la seva demostrada eficiència al llarg dels darrers anys amb les cadenes de blocs més importants.

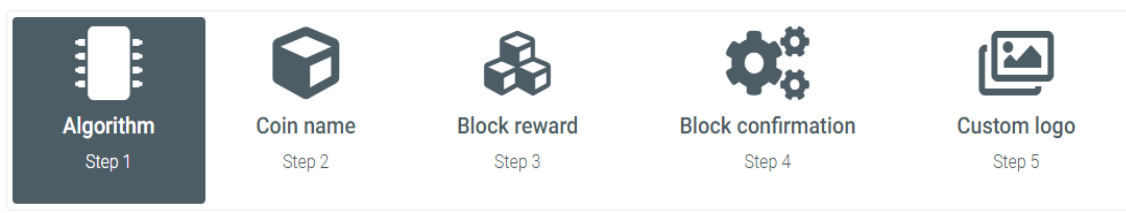
<i>Proof of Work</i>	<i>Proof of Stake</i>
Per a la creació de blocs, cal solucionar problemes matemàtics amb processadors informàtics	El creador del bloc és un propietari de la criptomoneda seleccionat per un algoritme
Es recompensa amb criptomonedes noves als miners que creen el bloc	Les recompenses són proporcionades per les comissions de transacció de la xarxa
Per a unir un bloc manipulat, cal tenir més del 51% del poder computacional de tota la xarxa	Només es pot incloure blocs manipulats si es té en propietat més del 51% de totes les existències de la criptomoneda
<i>Bitcoin i Ethereum Actual</i>	<i>Ethereum 2.0</i>

Taula 1. Elaboració Pròpia. 2021. Diferències entre Proof of Work i Proof of Stake

Una vegada coneguda la teoria sobre aquesta tecnologia, es podria arribar a pensar que la seva aplicació compta amb un component insuperable de dificultat, si més no, res més lluny de la realitat. Tot i que el back office de l'arquitectura tecnològica està format per aspectes complexos com la criptografia mencionada, la posada en pràctica és extremadament senzilla gràcies als programes desenvolupats per enginyers informàtics que els posen a l'abast de tot el món. Com passa amb els rellotges suïssos, la seva extrema dificultat d'enginyeria per a la precisió temporal no exclou que sigui fàcil d'entendre la seva funcionalitat per a marcar els dies i les hores amb simples agulles.

És prou raonable que les organitzacions hagin desenvolupat interfícies gràfiques que deixen un nivell de dificultat ínfim per als usuaris, però aquesta facilitat és aplicable a tots els aspectes de la *Blockchain*, com es demostrarà a continuació, ja que per a exemplificar-ho es durà a terme una creació complerta d'una cadena de blocs, juntament amb la mineria de la seva criptomoneda pròpia únicament amb finalitat educativa.

Inicialment, farem ús d'un *software* de codi obert per a tothom qui el vulgui utilitzar o modificar, anomenat Wallet Builders, traduït literalment com a constructors de carteres. El procediment és ben senzill, demanant dades essencials per a la creació de la cadena de blocs, repartits en cinc etapes de creació.



The interface shows five steps for creating a wallet:

- Algorithm** (Step 1): Represented by a circuit icon.
- Coin name** (Step 2): Represented by a cube icon.
- Block reward** (Step 3): Represented by three stacked cubes icon.
- Block confirmation** (Step 4): Represented by two interlocking gears icon.
- Custom logo** (Step 5): Represented by a document with a picture icon.






Below the steps, there are input fields for:

- Email address**: A text input field with a placeholder "Email".
- Coin type**: A dropdown menu with "Free" selected. Below it, a note says "Select a free or paid coin."
- Coin algorithm**: A dropdown menu with "Script - Proof of Work" selected. Below it, a note says "Select the algorithm for your coin."

Per a aquest exemple, escollim un algoritme de consens basat en la *Proof of Work* explicada anteriorment, ja que és el protocol escollit per les criptomonedes més exitoses i consolidades actualment, com és el cas del *Bitcoin* o l'*Ethereum*.






És tant elevat el component de personalització disponible a la creació d'aquests actius electrònics que permet una adequació excel·lent a cada projecte en particular, però en aquest cas, inicialment només es personalitzaran alguns aspectes com el nom de la criptomoneda anomenada UABCoin, la seva abreviatura per a les futures cotitzacions establerta en \$UAB, dient-li TFG a la unitat monetària més petita, i relacionant-la amb la pàgina web institucional per a més dades sobre el projecte.

Com a curiositat, al estar creant des de zero la cadena de blocs, s'obté el privilegi de poder inscriure-hi una frase al bloc Gènesi de la cadena, el primer de tots, conegut com a bloc 0 i actuant com a primera pedra si ho extrapoléssim al món de la construcció. En aquest cas, s'ha considerat interessant establir els valors del projecte, inscrivint-hi l'eslògan de la nostra universitat, *Audàcia del Coneixement a la Universitat Autònoma de Barcelona*.






 Algorithm Step 1	 Coin name Step 2	 Block reward Step 3	 Block confirmation Step 4	 Custom logo Step 5
--	--	---	--	--

Coin name	<input type="text" value="UABCoin"/>	✓
Name for your coin.		
Coin abbreviation	<input type="text" value="UAB"/>	✓
Abbreviation for your coin.		
Address letter	<input type="text" value="1"/>	▼
Starting letter for your public address.		
Coin unit	<input type="text" value="TFG"/>	✓
Name of the smallest unit for your coin.		
Timestamp	<input type="text" value="AUDACIA DEL CONEIXEMENT A LA UNIVERSITAT AUTONOMA DE BARCELONA"/>	✓
Unique sentence that is stored inside your genesis block.		
Website URL	<input type="text" value="https://www.uab.cat/"/>	✓
URL in about dialog of your coin that points to your website.		

En relació als aspectes tècnics sobre la oferta d'aquesta criptomoneda, s'ha considerat adequat seguir l'arquitectura de *halvings* empleada pel *Bitcoin*, ja que aporta un component de complexitat a la seva creació alhora que controla possibles inflacions que perjudicarien a les futures generacions d'estudiants. Per tant, s'estableix una *Supply* màxima de 30.000 unitats monetàries, establerta ja que tocarien a una mitja d'un UABCoin per a cada estudiant segons els gairebé 30.000 estudiants amb els que compta la nostra universitat, facilitant les transaccions al evitar els càlculs amb molts decimals. Aquesta oferta de monedes serà repartida en 100 monedes per cada bloc creat mitjançant el consens del *Proof of Work*, reduint aquesta recompensa a la meitat cada 150 blocs creats, els anomenats *halvings* que caracteritzen la conservació de valor del *Bitcoin*, imitant les fortaleeses del seu protocol però adaptant-lo a les necessitats de cada projecte.

 Algorithm Step 1	 Coin name Step 2	 Block reward Step 3	 Block confirmation Step 4	 Custom logo Step 5
Block reward				
<input type="text" value="100"/> ✓				
Number of coins received for mining a block with Proof of Work.				
Block halving				
<input type="text" value="150"/> ✓				
Block halving splits the block reward in half.				
Coin supply				
<input type="text" value="30000"/>				
Total number of coins your coin will create.				

Eines com aquesta donen l'opció d'optimitzar la criptomoneda tant com puguis segons el projecte al que estigui relacionada, amb variables complexes d'establir com el temps establert abans de que es reajusti la dificultat de l'algoritme del *Proof of Work*. Tot i que és positiu el fet de comptar amb aquestes variables, el mateix *software* et proporciona una configuració per al correcte funcionament del protocol, donant per defecte dades plenament funcionals, facilitant la implementació d'aquests sistemes. Finalment, la criptomoneda producte d'aquest procediment es pot personalitzar tant com vulguin els creadors, des d'un logotip per a identificar-la fins a descripcions del projecte, entre altres opcions.

 Algorithm Step 1	 Coin name Step 2	 Block reward Step 3	 Block confirmation Step 4	 Custom logo Step 5
---	---	--	---	---

Coinbase maturity

Number of blocks before a mined block can be spend.

Number of confirmations

Number of blocks before a transaction is confirmed.

Target spacing in minutes

Number of minutes it should take to mine a block.

Target timespan in minutes

Number of minutes before difficulty of the network is re-adjusted.

☒ Hardcoded node

Your wallet will automatically connect with a hardcoded node.

Node 1

Hostname/IP of server that will run a node for your coin.

Node 2

Hostname/IP of second server that will run a node for your coin.

Una vegada arribat a aquest punt, ja es disposa del codi font que recull totes les complexitats tecnològiques de la nova cadena de blocs, creada amb característiques avançades com són els algoritmes de *Proof of Work* i els *halvings*, optimitzant-la per a la seva implementació a la universitat.

Coin properties

Compiling OS	Ubuntu 18.04 LTS	Advanced properties	
Source branch	0.18	Coinbase maturity	20 (+ 1 default confirmation) blocks
Algorithm	Script Proof of Work	Target spacing	5 minutes
Coin name	UABCoin	Target timespan	10 minutes
Coin abbreviation	UAB	Transaction confirmations	6 (+ 1 default confirmation) blocks
Public address letter	1	Timestamp	AUDACIA DEL CONEIXEMENT A LA UNIVERSITAT AUTONOMA DE BARCELONA
RPC port	35849	Node 1	node2.walletbuilders.com
P2P port	35850	Last block with reward	5100
Block reward	100 coins	Time until last block	0 years, 0 months, 17 days, 17 hours
Block halving	150 blocks		
Coin supply	30000 coins		
Website URL	https://www.uab.cat		

Ja només queda el procés de mineria de la criptomoneda, creant noves unitats explotant l'algoritme del nostre actiu, un procediment dut a terme mitjançant el primer node integrat a la cadena de blocs que actuarà a través d'una cartera creada específicament per a la UABCoin, tot això amb procediments gairebé automàtics com es mostra a continuació, necessitant únicament un ordinador amb prestacions habituals a la societat actual. Primer, caldrà descarregar la cartera digital creada alhora que la nostra moneda pel propi codi de programació, un lloc on poder emmagatzemar inicialment la criptomoneda quan sigui minada.



Per a que aquesta *wallet* es sincronitzi automàticament amb el node assignat a la UABCoin, només caldrà crear un arxiu al directori de la cartera amb la següent informació, establint connexió entre el node preparat per a la mineria i la cadena de blocs on haurà de dur a terme l'algoritme del *Proof of Work*.



*UABCoin.conf: Bloc de notes

Archivo Edición Formato Ver Ayuda

```
rpcuser=rpc_UABCoin
rpcpassword=pifw1fqxfkdd23n59rcr63sqrfiqkw184uxb0blo
rpcallowip=127.0.0.1
listen=1
server=1
addnode=node1.walletbuilders.com|
```

Posteriorment, caldrà establir el codi que activi i desactivi la funció de mineria al nostre node, enviant-li les ordres per a que inici la mineria del bloc gènesis de la nova *Blockchain* anomenada UABCoin.

37.97.179.18:35850 (nodo: 1) via 83.53.199.253:64740	
En la lista blanca	No
Dirección	Saliente
Versión	70015
User Agent	/UABCoinCore:1.0.0/
Servicios	NETWORK & BLOOM & WITNESS
Importando bloques...	1
Sincronizar Cabeceras	1
Bloques Sincronizados	1
Puntuación de bloqueo	0
Duración de la conexión	10 m 8 s
Último envío	7 s
Última recepción	7 s
Enviado	937 B
Recibido	913 B
Ping	40 ms
Espera de Ping	N/D
Ping mín.	40 ms
Desplazamiento de tiempo	0 s




mine.bat: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
@echo off
set path_cli=%cd%
cd %path_cli%
echo Press [CTRL+C] to stop mining.
:begin
UABCoin-cli.exe generate 1
goto begin
```

Finalment, caldrà executar l'algoritme de mineria des del codi de programació vinculat a la cartera, donant inici a la història de la nostra cadena de blocs amb la creació del seu bloc Gènesis, on hi serà inscrit per sempre *l'Audàcia del Coneixement a la Universitat Autònoma de Barcelona*, obtenint els primers 100 UABCoins en tan sols 10 minuts des de la seva creació, convertint-se en una cadena de blocs plenament funcional per al benefici de la nostra universitat.

Transacciones recientes



21/05/2021 21:33

(WoccrL6cs6Diw97Ab5J4vMs9J3BGMDFyh)

[+100.00000000 UAB]

Node hosting

Status	Online
Block height	4
P2P connections	1
Network difficulty	0.000244137132
Network hashes per second	0.0455 kH/s
Last mined block	40 seconds ago



A partir d'aquest punt, amb una criptomoneda amb totes les capacitats transaccionals ja habilitades gràcies al primer node, caldria afegir-hi fonaments interessants al projecte per a que realment compti amb valor, reunint a més usuaris interessats en les seves característiques que actuarien com a nodes, podent portar a la nova criptomoneda a cotitzar segons la seva demanda relacionada amb la oferta disponible.

S'hi podrien implementar tantes finalitats com sigui capaç d'imaginar la societat, utilitzant-la com a pagament intern a les facultats de la universitat lligant-la al carnet de l'estudiant que actuaria com a cartera, i permetent beneficis als propis alumnes de la universitat ja sigui tant amb serveis com el de fer el pagament a la cafeteria o a les màquines fotocopiadors, aquestes darreres actualment funcionant amb un sistema que necessita prepagament en efectiu centralitzat a una màquina física a les instal·lacions sovint avariada o ocupada per altres usuaris. També hi ha altres alternatives basades en la traçabilitat, aplicant-la als milers llibres en préstec de les grans biblioteques de la Universitat Autònoma de Barcelona, fins i tot podent integrar un sistema interuniversitari per a l'enriquiment del coneixement de tots els estudiants, habilitant la nostra criptomoneda a les transaccions digitals aplicables a tot l'ecosistema al que es desitgi implementar.

En conclusió, aquesta és una perfecta exemplificació didàctica per a demostrar que l'ús de la tecnologia *Blockchain* és completament assolible per al públic generalista de la població, adoptant una forta accessibilitat que és indispensable per a la seva erupció i consolidació als diferents sectors de la societat.

Després d'aquests passos relativament senzills pel que suposa la creació d'una criptomoneda amb arquitectura *Blockchain* tant complexa, ja comptem amb l'actiu basat en la nostra pròpia cadena de blocs, una configuració i implementació que amb els sistemes tecnològics establerts a la actualitat estaria valorada en milers d'euros per un sistema de característiques més limitades, obrint-nos un gran ventall de possibilitats amb la creació de la UABCoin, la nostra pròpia criptomoneda. Tecnològicament és una criptomoneda amb una complexitat tan elevada com les més exitoses i establertes al mercat, però amb una senzillesa de creació que obre aquesta tecnologia a tota la població, un factor clau per a la seva disrupció.



Il·lustració 5. Elaboració Pròpia. 2021. Logotip de la Criptomoneda UABCoin

3. ANÀLISI DEL POTENCIAL ASSOLIBLE AMB TECNOLOGIA *BLOCKCHAIN*

Com s'ha mostrat anteriorment, la capacitat de les cadenes de blocs és tan immensa que a la pràctica serà tan gran com l'interès i inversions que es generin als diferents sectors on seria beneficiosa la seva aplicació, els quals s'explicaran detalladament a continuació, mostrant com la tecnologia *Blockchain* ja és un component real a la societat d'avui en dia.

3.1. NOVES RELACIONS CONTRACTUALS AMB ELS *SMART CONTRACTS*

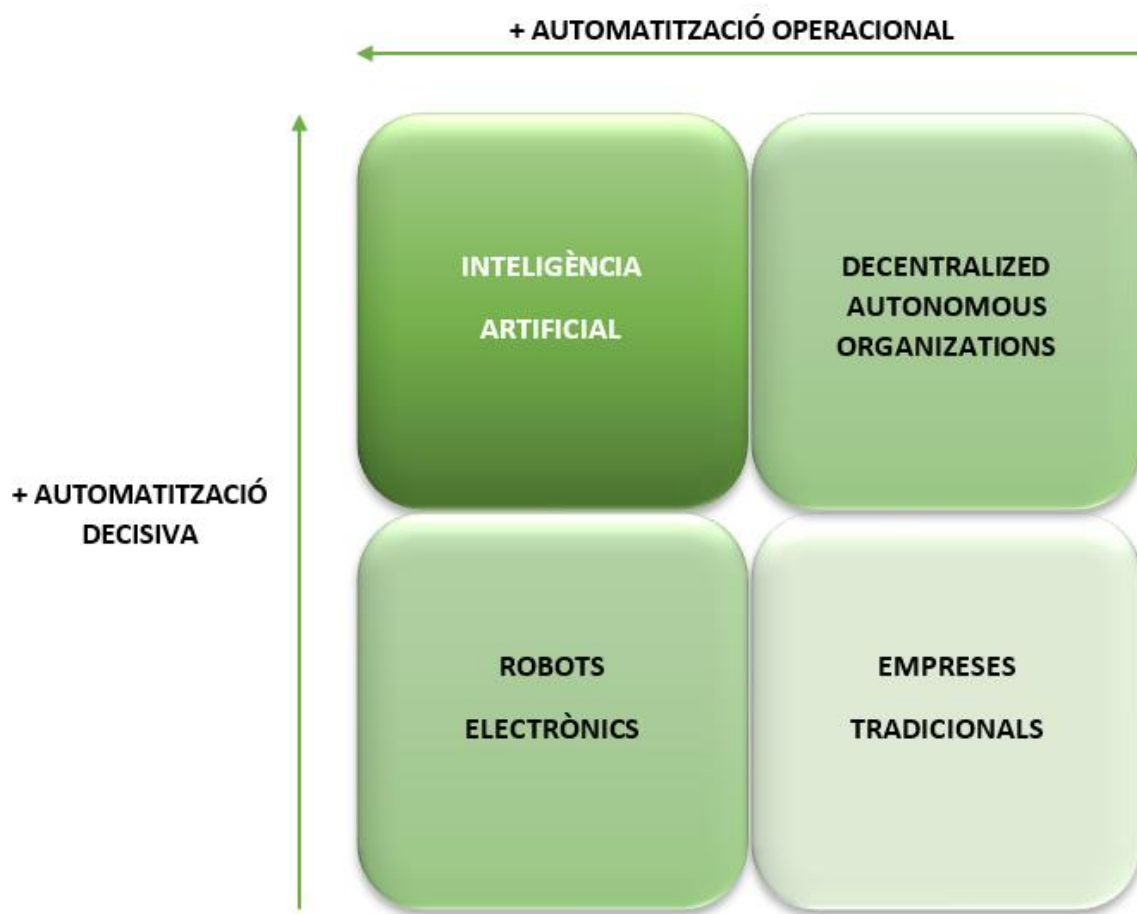
Els contractes intel·ligents presenten un gran avantatge respecte als tradicionals, ja que passen d'una posició inerta i passiva cap a l'adopció d'una responsabilitat dinàmica, no només definint les condicions contractuals aplicables a les parts implicades, sinó que la innovació permet automatitzar des del seguiment fins al compliment de les condicions establertes al contracte juntament amb un sistema de liquidació monetària entre les parts plenament integrat, permetent reduir pèrdues econòmiques al minimitzar les despeses per judicis en casos de malentesos o mala fe, actuant el contracte de manera ininterrompuda adherint-se les condicions establertes, sense cap mena de frau ni interferències durant la seva vigència contractual.

Els *Smart Contracts* habitualment són allotjats a la *Blockchain* d'*Ethereum*, actualment la principal criptomoneda alternativa al *Bitcoin*, sent reconeguda com a la *altcoin* capdavantera, un terme utilitzat per a les *alternative coin* més enllà de la precursora que s'han anat desenvolupant des de les arrels establertes pel codi obert de Satoshi Nakamoto però amb diversos matisos per a cada cas, com major facilitat per a la creació de nous blocs o diferents protocols algorítmics, generant un ventall d'alternatives adaptables a les necessitats de cada usuari.

Aquesta autonomia contractual ha donat lloc a solucions digitals com les creixents Organitzacions Autònomes Descentralitzades, també conegudes com a *DAO* pel seu acrònim de l'anglès, generant una organització documental basada en l'estructura de *Smart Contract*, assolint característiques beneficioses com la transparència i la incorruptibilitat degudes a la automatització i descentralització relacionades a aquesta nova tecnologia.

Les *DAO* varen ser impulsades pel posteriorment cofundador d'*Ethereum*, Vitalik Buterin, als voltants de l'any 2014 i des de llavors no ha cessat la seva popularització basada en la descentralització institucional, deixant de ser un element necessari la formalització d'empreses mitjançant entitats governamentals, obrint un món d'oportunitats al ser allotjades a la pròpia cadena de blocs en forma de *Smart Contract* i proporcionant totes les característiques d'automatització lligades a aquests elements, que seran detallades posteriorment.

Dins d'aquest nou escenari s'eliminarà la necessitat del consell d'administració i altres posicions jeràrquiques amb grans costos associats simplement per aprovar decisions, ja que cadascuna de les decisions empresarials seran preses segons les directrius del codi informàtic introduït als contractes intel·ligents sempre que hi hagi consens entre els propietaris o accionistes de la *DAO*, minimitzant el risc associat al factor humà tant per errades procedimentals com per ineficiències emocionals durant la gestió, les quals no afectaran al negoci gràcies a la automatització generalitzada menys en aquells moments on sigui estrictament necessària la participació humana a nivell operatiu, ja que la presa de decisions és plenament autònoma.



Il·lustració 6. Elaboració Pròpia. 2021. Matriu d'Automatització Empresarial

Dins de l'estructura organitzativa, tots aquells usuaris que disposin de *tokens* emesos en un principi a la *Initial Coin Offering* que serà detallada més endavant o comprant-los posteriorment a preu de mercat, adquiriran certs privilegis com el poder de decisió dins de l'entitat o l'obtenció de beneficis mitjançant dividends entre d'altres, al ser parcialment propietaris del projecte. Les condicions contractuals seran acordades segons les característiques establertes per a cada *Decentralized Autonomous Organization* amb una potent fortalesa de seguretat i reducció de costos, juntament amb un augment d'eficiència molt considerable respecte a estructures empresarials habituals.

Tot i que sobre el paper sembli que la balança s'inclina a favor de l'establiment de les *DAO*, és essencial i necessari considerar els perills derivats de possibles carències de seguretat per part dels programadors del projecte informàtic, mitjançant complexos algoritmes que en cas de presentar debilitats podrien posar temporalment en perill la integritat del projecte, tot i que posteriorment es puguin recuperar les dades al estar allotjada a la cadena de blocs, com ja va passar amb el projecte *The DAO* a l'any 2016 amb el robatori mitjançant un *hack* que va aconseguir integrar-se a la *DAO* retirant gairebé 40 milions de dòlars que varen ser íntegrament recuperats gràcies a les característiques mencionades del *Blockchain*, però sense evitar la desconfiança i preocupació dels inversors envers la vulnerabilitat de les *Decentralized Autonomous Organization* que restaria els beneficis d'una de les principals característiques associades als beneficis de les cadenes de blocs.

Addicionalment, caldrà valorar i donar importància als perills d'estafa dins d'aquest model estructural, al no estar emparat sota les proteccions reglamentàries governamentals que protegeixen als inversors envers negocis fraudulents.

Una altra aplicació destacable dels contractes intel·ligents és el fet d'establir en el present certes condicions que s'activarien en un futur si es compleix certa condició, eficientment aplicable al matrimoni, ja que s'evitarien un enorme nombre de conflictes si una parella estableix les condicions de divorci i custòdia en un moment en que ambdós estiguin bé sentimentalment, sense personalitats venjatives que provoquin acusacions distorsionades per cap de les parts.

Òbviament, això és plenament extrapolable a les relacions professionals, ja aplicable a la actualitat entre empreses que s'acullen a la eficiència de les innovacions mitjançant la implementació progressiva dels contractes intel·ligents a les relacions laborals.

Dins del gran ventall d'oportunitats que generen els *Smart Contracts*, podem trobar-ne aplicacions amb millores d'eficiència molt destacables, com és el cas de les exportacions amb contractes condicionats a demores de transport intercontinentals, permetent executar automàticament els pagaments en quant es tingui constància a la cadena de blocs de que es compleixen les condicions contractuals establertes.

Per exemple, quan un vaixell ple de contenidors de mercaderia tecnològica viatgi des del continent asiàtic cap als Estats Units, acordant contractualment ambdues parts que el pagament únicament es duria a terme si la mercaderia importada es descarrega al port de Los Ángeles, una contracte intel·ligent a la cadena de blocs podrà generar la possibilitat d'automatitzar el pagament ja que en quant s'informi de la descàrrega de mercaderies al destí, i una vegada comprovades automàticament les relacions contractuals establertes com el document del *Bill of Landing*, s'haurà complert la condició necessària del contracte i activarà automàticament l'execució del mateix, sense demores ni ineficiències.

Aquesta és una disrupció tecnològica alternativa als crèdits documentaris que proporcionen actualment les entitats bancàries, evitant el sobre cost que comporta la intermediació gràcies a les propietats aportades pels *Smart Contracts*.

3.2. DAPPS PER A UNA ECONOMIA COL-LABORATIVA REAL

Cal destacar que l'aparició dels contractes intel·ligents també ha creat una oportunitat d'innovació basada en els mateixos com és el cas de les *DApps*, acrònim traduït d'Aplicacions Distribuïdes, un element d'enginyeria de *software* que té totes les característiques necessàries per a ser el nou substitut de les pàgines web. La principal diferència resideix a l'arquitectura informàtica, ja que mentrestant les interfícies de programació d'aplicacions habituals necessiten connectar-se a una base de dades tradicional, les *DApps* fan aquest procediment connectant-se a *Smart Contracts* per a l'obtenció d'informació que es mostrarà a l'usuari.

Un cas pràctic ja en funcionament al nostre país és la plataforma Finweg de Bankia, la qual mitjançant *Smart Contracts* permet detallar el procés de pagament per a cadascuna de les parts contractualment involucrades, tot i que actualment està entrant al mercat en una versió limitada únicament a contractes transaccionals entre empreses, és a dir *B2B*, però ja compta amb un complex sistema de certificadors que aporten seguretat al procediment a favor dels diversos agents contractuals.

Una de les opcions generades per aquesta aplicació és la creació de pagaments condicionats, obtenint un extra de confiança al ser un procediment automatitzat i verificable segons el compliment de les condicions contractuals, podent realitzar cobraments i pagaments organitzadament mitjançant la seva plataforma establerta a la cadena de blocs.

Per altra banda, les grans empreses revolucionaries dins del seu sector com Glovo o Cabify es protegeixen de la opinió social darrera d'una publicitat en forma d'economia col·laborativa, tot i que res està més lluny de la realitat.

El seu model de negoci es basa en addicionar treballadors autònoms per a revendre els seus serveis, amb les grans empreses com a principals retenidors de valor al ser els poderosos intermediaris que cobren comissions d'intermediació i es queden amb dades d'usuaris altament valuoses per a la seva explotació als mercats actuals, obtenint encara més beneficis posteriorment mitjançant publicitat entre d'altres.

“En comptes de treure el lloc laboral a un taxista, la tecnologia Blockchain se'l treu a intermediaris com Uber i obre pas a un negoci directe entre el professional i el client”, com bé defensa el fundador d'*Ethereum*, Vitalik Buterin.

Gràcies a les característiques que aporta el protocol lligat a la cadena de blocs mitjançant les *Distributed Apps*, ja és possible veure aplicacions d'economia col·laborativa real, amb un format empresarial similar a les cooperatives tradicionals ja que són propietat dels membres que la formen, però amb el gran benefici de que l'aplicació amb tecnologia *Blockchain* permet cercar dins de la cadena de blocs aquelles opcions que millor s'adaptin a cadascun dels usuaris, creant en un ecosistema sense comissions d'intermediació i obrint un extens ventall de possibilitats com són les posteriors ressenyes dels clients, permetent la verificació de que cada client tingui dret a valorar únicament aquells serveis dels que realment n'ha fet ús i comptant amb un sistema integrat de pagaments mitjançant les pròpies criptomonedes, amb tots els beneficis mencionats anteriorment que això comporta.

Superficialment, les interfícies de les aplicacions basades a la cadena de blocs podria ser exactament igual que la de les aplicacions populars avui en dia, però amb una arquitectura tecnològica darrera de cada procediment que augmenta notablement la eficiència i experiència dels usuaris, passant d'una interacció amb un tercer cap a una relació entre iguals gràcies al potent *back office* tecnològic.

Aquesta millora es notaria certament en aspectes concrets de cada treball, ja sigui des de conductors que reben del propi client el trajecte exacte que volen recórrer fins a repartidors que reben la comanda directament de l'usuari beneficiant-se de tot el preu del servei, evitant escenaris d'explotació laboral per part dels empresaris ja que ara el poder és repartit de manera homogènia, d'igual a igual, sempre podent consultar la identitat inalterable i reputació de cadascuna de les parts, optimitzant en conjunt la relació dels usuaris, beneficiant-se ambdues parts.

Per tant, el potencial assumible és immens, sobretot considerant que la majoria de cadenes de blocs són sistemes lliures de codi obert, és a dir que facilitant el codi font sobre el qual està dissenyat el *software* obren la innovació i col·laboració a cadascun dels usuaris mitjançant còpies on poder experimentar amb modificacions personalitzades, pel que es podran dur a terme grans avenços dins de la estructura de la tecnologia *Blockchain*.

Aquest és un fet que ja va succeir amb comunitats de diferent naturalesa com va ser-ho en el seu moment amb les aportacions de la població als articles de *Wikipedia*, unes plataformes gairebé impossibles d'aconseguir dins dels sectors privats però assumibles amb la participació d'un gran nombre d'usuaris amb la mateixa posició de poder, un interès cap a les aportacions que a més a més augmentaria notablement, ja que es podrien recol·lectar remuneracions proporcionals al valor creat per cada usuari dins de les bases de dades distribuïdes, gràcies a la traçabilitat i reputació de les seves aportacions.

Tot i ser una tecnologia popularment coneguda per la seva aplicació orientada cap a les criptomonedes, compta amb un extens ventall de possibles aplicacions en continua expansió, creant valor de processos transaccionals completament diversos.

3.3. MILLORA D'EFICIÈNCIA AL SECTOR ASSEGURADOR

La *Blockchain* també tindrà un creixement exponencial en condicions peculiars com la del sector assegurador. Actualment és habitual comptar amb demores i mals de cap a l'hora de reclamar el cobrament de sinistres inclosos a les pòlisses signades amb entitats asseguradores, no per mala fe de les empreses, sinó per la dificultat de valorar dinàmicament cadascun dels casos sinistrats amb característiques habitualment heterogènies entre clients. La dificultat de valoració encara és més important amb la gran varietat de productes asseguradors que es troben avui en dia al mercat i compten amb diferents cobertures, podent comparar-les totes elles amb buscadors que prioritzen les opcions més econòmiques per al consumidor augmentant el nivell de competència entre empreses, juntament amb el sorgiment d'entitats asseguradores basades en la digitalització amb notables beneficis d'eficiència gràcies a la adopció de les tecnologies més avantguardistes com l'ús del *Big Data* o la pròpia *Blockchain*, les anomenades *Insurtech*.

Per a la millora d'aquest sector caldrà comptar amb les cadenes de blocs, ja que si amb cada client es formalitza un *Smart Contract* on s'estableixin les condicions contractuals especificant les cobertures de la pòlissa, automàticament en quant es tramiti un sinistre es procedirà al pagament de la quantitat establerta entre ambdues parts, com podria ser amb les assegurances de vida o de decessos en quant s'informa adequadament de la defunció de l'assegurat, procedint al pagament automatitzat a favor del beneficiari i evitant demores o ineficiències humanes gràcies al contracte intel·ligent, homogeneïtzant en una mateixa cadena de blocs tots els procediments administratius necessaris permetent fer un anàlisi i seguiment de cadascuna de les tramitacions de sinistres, una millora que a més a més de reduir els costos suposarà una minoració al temps de tramitació, beneficiant tant a les empreses com als propis assegurats.

Dins del sector assegurador, ja hi ha en marxa diversos consorcis formats per les entitats més establertes al sector però que els hi sorgeix la necessitat d'adaptar-se als nous temps a través de la investigació de les cadenes de blocs i la possible adopció al seu negoci, com és el cas del Blockchain Insurance Industry Initiative B31 format per un conjunt de grans entitats com són les alemanyes Allianz i Zurich, entre d'altres.

Gràcies a aquesta implementació tecnològica, els productes proporcionats per les asseguradores cada vegada podran adaptar-se més a les necessitats dels clients, lligant les possibles ofertes de serveis asseguradors oferts amb les múltiples dades conegudes dels usuaris, com podria ser una assegurança de vehicles amb una prima completament lligada a les característiques del conductor i del cotxe, no només mitjançant qüestionaris, sinó amb la lectura de múltiples sensors que ja disposen alguns cotxes de gamma alta com és el cas dels elèctrics Tesla, cada vegada més populars, amb informació tant de l'estat del vehicle com de l'estil de conducció del seu propietari.

Cal destacar que aquesta unió de les múltiples dades del *Big Data*, amb la sensorització del *Internet of Things*, i els *Smart Contracts* de la tecnologia *Blockchain*, generen un paradigma completament nou dins del sector assegurador que si aconseguixen implantar-lo de manera generalitzada, elevarien a les entitats asseguradores cap a un nivell d'eficiència mai vist fins a l'actualitat.

3.4. SINÈRGIES AMB LA *INTERNET OF THINGS*

Com s'ha vist fins a aquest punt, la tecnologia *Blockchain* es veu inclosa en un moviment disruptiu i revolucionari que es retroalimenta entre avenços digitals per al benefici del conjunt de la societat, habilitant això el seu creixement gràcies a la disminució de la reticència al canvi que van presentant els usuaris al adonar-se'n de que el món es troba en un cicle de continues adaptacions a l'entorn.

Tot i així, la confiança en la tecnologia es un factor clau a treballar, reduint aquesta reticència al canvi que genera la naturalesa humana. Davant un futur amb múltiples dispositius intel·ligents que administrin dades útils per a la humanitat, amb tan amplies aplicacions com podria ser des del seguiment de les constants vitals d'una persona fins a la comprovació de l'estat d'infraestructures a temps real, caldrà tenir en compte que per a afrontar un *Internet of Things* s'haurà de comptar amb un *Register of Things* que tingui la capacitat transaccional i computacional suficient per a afrontar tal desafiament, sent això possible gràcies a les capacitats de les cadenes de blocs unides a protocols transaccionals que enviïn les dades des dels objectes intel·ligents.

Unint a ambdues tecnologies, la *Blockchain* i la *Internet of Things*, obtenim una xarxa coneguda com a *mesh network* capaç de revolucionar els diversos sectors professionals amb solucions que fins avui en dia ens semblen d'un futur llunyà, però realment són a tocar.

Un exemple amb molta utilitat és la comunicació sobre el seu estat i integritat per part dels objectes, des de xarxes telefòniques o canonades del clavegueram fins a les pròpies edificacions o carreteres, entre moltes altres opcions.

Gràcies a les noves tecnologies, amb la sensorització d'objectes es pot aconseguir que ells mateixos, de manera autònoma, identifiquin les incidències en el seu ús normal i previnguin possibles complicacions causades per deterioraments invisibles als ulls humans però detectables mitjançant sensors, comunicant-ho de manera automàtica a la xarxa de vigilància juntament amb les seves dades d'ubicació per a millorar exponencialment la eficiència dels tècnics encarregats del seu manteniment.

Amb una gran quantitat de productes quotidians que cada vegada és més habitual que estiguin interconnectats amb aplicacions i bases de dades, com són els productes d'electrònica anomenats *smart*, la personalització dels serveis que ofereixen tant televisors com servidors de *streaming* entre d'altres és una grandíssima avantatge que millora l'experiència dels usuaris envers els serveis oferts.

Aquestes noves connexions dels objectes, incloent electrodomèstics que fins ara consideraríem tradicionals com neveres o la domòtica de les llars, també justifiquen l'augment exponencial de la quantitat de dades que es mouen a les xarxes, juntament amb la popularització de grans receptors de dades que fins ara no podrien ser captades en quantitats tan grans, com les polseres d'activitat *Mi Band* de *Xiaomi* o la domòtica amb *Alexa* d'*Amazon*, actuant com a sensors captadors de dades que podrien introduir-se a la cadena de blocs per a la seva explotació a favor de l'usuari.

Aquesta unió tecnològica també podrà tenir una utilitat destacable cap al compliment de les lleis, com és el cas d'enregistrar immutablement la velocitat dels vehicles relacionant-ho amb la seva geolocalització, detectant immediatament infraccions perilloses per a la societat, o fins i tot amb sensors encarregats de denegar la funció del motor d'arrencament en aquells vehicles que no tinguin una situació regularitzada dins de la suposada *Blockchain* de la policia, evitant la circulació de vehicles sense assegurança o inspeccions tècniques que resultin perillosos per a la resta de ciutadans.

L'augment significatiu de dades sobre els objectes també afectarà a sectors tant diversos com el detallat anteriorment de les assegurances, ja que comptant amb un gran nombre de dades serà molt més precisa l'estimació de la quantitat monetària de prima necessària segons els seus estudis actuàrials, calculats amb un major nombre de variables recol·lectades que aportaran una precisió mai vista a les estimacions de riscos.

A més a més, aquestes noves interconnexions ens proporcionen cobrir necessitats que fins ara no havien sigut tractades de manera eficient per cap producte al no tenir les tecnologies necessàries, com és el control sanitari a distància, ja que actualment es poden controlar remotament les constants vitals i altres factors de pacients sense haver d'estar físicament propers ni en la mateixa ciutat.

Aquest gran avenç s'aconsegueix mitjançant objectes intel·ligents connectats mitjançant les xarxes a dispositius controladors, augmentant notablement la qualitat de vida de persones dependents o en grups de risc. Per exemple, una clara millora social aportada per la tecnologia és el cas de poder mantenir un control constant de la glucosa per a pacients amb diabetis mitjançant un sensor adhesiu situat per sobre de la pell, un mètode gens intrusiu que pot evitar problemes de glucèmia amb greus conseqüències, tant per al propi pacient com per familiars encarregats de cuidar-lo en casos d'invalidesa, juntament amb moltes altres alternatives aplicables a malalties de diverses característiques.

Definitivament, gràcies a les característiques detallades anteriorment d'aquesta tecnologia disruptiva, són notables les sinèrgies entre *Blockchain* i el conjunt de la *Internet of Things*.

3.5. EL VALOR DE LES DADES, BENEFICI DE LA POBLACIÓ MUNDIAL AMB *DEFI*

Ens trobem en una situació cibernètica on cada vegada hi ha menys intimitat a causa dels tercers implicats a la xarxa, com s'ha demostrat amb la creixent conscienciació cap a l'ús adequat de les *cookies* i dades recol·lectades per empreses externes durant les cerques a internet.

Per aquest motiu, la implementació d'una tecnologia *Blockchain* on es mantingui plenament la privacitat sense la presència de tercers amb més seguretat contra les creixents amenaces de delinqüència a la xarxa i sense perdre cap privilegi dels que ens aporta la tecnologia, és un nou paradigma al que molts dels usuaris miren amb bons ulls.

A més a més, el fet de tenir bases de dades descentralitzades a nivell mundial permetrà reduir notablement els costos associats a les recerques tant de dades com d'altres aspectes buscats per les indústries actuals, com és el talent professional, comptant amb xarxes que juntament amb la seva interrelació entre entrades, permetran obtenir resultats de recerques amb historials de transaccions entre registres fiables, podent filtrar diferents camps tant d'usuaris com d'empreses a nivell mundial.

Aquest és un sistema de motor de recerca que aconsegueix plantar cara al model de Google per l'augment d'eficiència amb la major interrelació i fiabilitat de dades permanentment registrades, cercant des de la privacitat evitant la creació de *cookies* amb informació dels usuaris, tot i que òbviament aquest model encara es troba molt lluny del gegant tecnològic, el qual podria adoptar aquesta tecnologia en quant es senti amenaçat per la mateixa.

Les cadenes de blocs, juntament amb la confiança que generen, podran donar lloc a millores amb efectes directes sobre la humanitat. Per exemple, es veuria exponencialment augmentat el nombre de donants a favor de les Organitzacions No Governamentals sempre que es pogués seguir i verificar la finalitat de cada donació, generant un augment de confiança cap a organitzacions sense ànims de lucre que cada vegada es veuen més rodejades de polèmiques.

Un altre terme altament interessant és la Identitat Digital Sobirana, creant un perfil personal establert a la cadena de blocs amb dades personals privades per que els ciutadans puguin interactuar les empreses, però preservant sempre la seguretat i privacitat ja que segons l'empresa a la que es destinin les dades personals se li proporcionaran unes o d'altres.

Per exemple, a gimnasos només els hi seria visible el nom i l'estat de salut de l'usuari, no cal tantes dades com demanen actualment. Aquest és un benefici destacable, sobretot amb la creixent consciència sobre la propietat i protecció de les dades personals.

Amb la implementació d'aquesta tecnologia, guanyarien un component de transparència i seguretat que seria essencial per a les aportacions de molts ciutadans, evitant la desviació de fons cap a intermediaris ja innecessaris, beneficiant-se finalment els més necessitats de la societat sense alteracions ni polèmiques, exposant davant la justícia als delinqüents que cometin malversacions de fons, i mostrant de manera transparent la feina d'aquelles organitzacions que fan del món un lloc millor.

La tecnologia descentralitzada permetrà també reduir les desigualtats que es pateixen al món per certes dades associades a les persones, evitant discriminacions segons l'origen dels usuaris i virant a favor d'un judici estrictament lligat a les característiques d'una identitat digital individualitzada amb dades reals i fidedignes.

Aquesta identitat permet mostrar únicament la informació rellevant per a cada procediment en concret i, consegüentment, sense limitacions per nacionalitat a l'hora de contractar serveis bancaris gràcies a la tecnologia de la cadena de blocs. Aquest és un gran pas endavant cap a la globalització i desenvolupament de països del tercer món, els quals es veuen limitats per discriminacions segons les seves dades geogràfiques, més enllà de les característiques dels projectes que presentin els emprenedors i empresaris del país.

Per exemple, molts empresaris denegarien el pagament dels seus productes o serveis mitjançant xecs bancaris amb origen centre-africà, però això passa a causa de la inestabilitat de les institucions bancàries de la zona, i no per la persona africana darrera de la transacció comercial que la cadena de blocs permetrà jutjar únicament per la seva identitat digital pròpia, al no dependre directament del seu país, sinó de les seves dades.

Per tant, descentralitzant les finances mitjançant els protocols de finances descentralitzades coneguts com a *DeFi*, la tecnologia *Blockchain* també obra una finestra a trencar el cercle de la pobresa ja que permet el seu us com a forma de finançament, considerant que al tercer món el capital és extremadament car amb grans interessos, i el necessiten per a activitats agrícoles d'exportació altament productives.

Actualment hi ha un gran marge de millora social amb finalitats ètiques a favor de la població de països en desenvolupament, intentant solucionar-se progressivament amb diverses plataformes ja en funcionament, a través d'un sistema organitzatiu categoritzat com a *crowdlending* social.

Ja existeixen casos reals amb aquesta finalitat, molt positius per a la població mundial, com és la plataforma espanyola EthicHub.

Mitjançant el seu sistema informàtic, a EthicHub aconseguixen posar directament en contacte a inversors d'arreu del món amb comunitats productores de països en desenvolupament, habitualment de cafè, que no tenen accés al sistema bancari amb condicions dignes sense tipus d'interès abusius, o que només poden comptar amb el finançament de grans empreses del sector que els hi cobrarien una comissió elevadíssima d'intermediació.

Amb aquesta connexió entre usuaris, els inversors aconseguixen arribar a projectes rentables i els agricultors aconseguixen finançament amb condicions adequades, beneficiant a ambdues parts amb un sistema de *crowdlending* amb efectes molt positius al conjunt de la societat.

Per tant, la tecnologia va molt més enllà del simple benefici comercial, tenint la capacitat d'alterar beneficiosament fins i tot els drets humans dels països amb població en situacions precàries, mitjançant un augment dels seus drets i capacitats dins del sistema financer.



Il·lustració 7. Esquema de la Plataforma Ethic Hub. 2021. Obtinguda de www.ethichub.com/

3.6. LES CRIPTOMONEDES, *BLOCKCHAIN* COM A MÈTODE TRANSACCIONAL

Dins del nou sistema financer generat per les cadenes de blocs, pren una importància essencial un nou actiu d'intercanvi i pagament lligat a aquesta tecnologia, les criptomonedes. Aquestes no són regulades per cap organisme governamental, un fet que podria generar desconfiança però que dins del sistema es considera com una gran avantatge, al ser diners electrònics descentralitzats sense sucumbir al poder de cap organisme superior, evitant les malversacions i intermediacions ineficients durant el flux monetari gràcies al sistema *peer-to-peer* de transaccions directament entre les carteres de les parts implicades, enregistrant-se cada moviment a una cadena de blocs completament infalsificable i inalterable per les propietats anteriorment detallades.

Un aspecte menys popularitzat de les criptomonedes és la seva possible actuació com a reserva de valor per al capital dels seus inversors, oferint una alternativa als utilitzats habitualment per a protegir el patrimoni de les possibles fluctuacions dels mercats de divises tradicionals com l'or o la plata, adquirint la capacitat de mantenir el seu valor al llarg del temps passi el que passi amb monedes com l'euro o el dolar.

Per a aquesta finalitat, és una condició necessària que l'actiu compti amb certes propietats, com és una durabilitat demostrada al llarg del temps per a evitar deterioraments, juntament amb una descentralització que no fa perillar la seva seguretat ni la seva integritat, i un component d'escassetat que eviti les depreciacions que succeirien al augmentar la oferta sobre la demanda.

Un actiu utilitzat com a reserva de valor és el cas del *Bitcoin*, amb una emissió màxima de 21 milions de monedes, atorgant-li una naturalesa afí a la deflació ja que l'oferta sempre serà finita. Per aquestes raons, alguns inversors consideren al *Bitcoin* el nou or digital, gràcies a les característiques que proporciona la tecnologia de la cadena de blocs.

Més enllà del positiu component de reserva de valor, i canviant de finalitat per a aquests actius digitals, és essencial prendre consciència de les limitacions actuals amb les que compten les criptomonedes com a mètode de pagament, ja que amb el valor monetari d'un *Bitcoin* al voltant dels 50.000 euros, la transacció per a la compra d'una peça de roba o un dinar podria comportar mirar xifres amb més de quatre decimals a causa del canvi *EUR/BTC*.

Una solució proposada per a simplificar aquest inconvenient matemàtic a la societat és la creació del Satoshi com a unitat monetària, dividint la mesura de valor amb un nom en honor al creador de la pròpia criptomoneda, sent aquesta la unitat indivisible del *Bitcoin* utilitzant el vuitè decimal com a unitat, és a dir, dividint el preu del *Bitcoin* entre 100 milions de vegades, obtenint quanties simplificades per a l'ús quotidià.



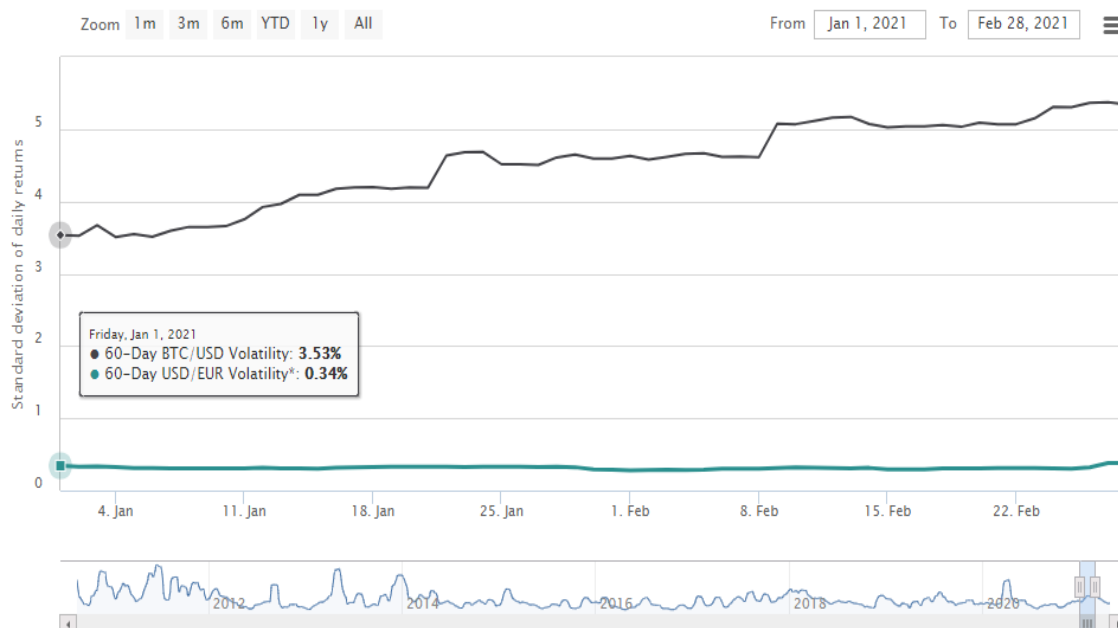
Il·lustració 8. 2021. Cotització del Bitcoin a CoinMarketCap. Obtinguda de <https://coinmarketcap.com/>

Tot i així, cal centrar-se en els problemes realment importants i amb solucions complexes que van més enllà de la simplificació matemàtica, com és el cas del gran component especulatiu lligat a les criptomonedes i la volatilitat extremadament elevada que les caracteritza, podent suposar un problema a la major part de la població, la qual des del desconeixement financer és essencial aporta'ls-hi estabilitat econòmica del seu poder adquisitiu, a més a més de necessitar un valor prou estable per a establir els preus dels béns que seran comprats per la població, sent un gran pas enrere pel sistema financer el fet de necessitar estar atent a la fluctuació del valor de la moneda pels grans canvis diaris, com succeeix a països com Veneçuela o Argentina amb hiperinflació causada per sistemes financers clarament precaris i ineficients.

Per tant, no és viable consolidar un sistema financer on amb uns estalvis d'una unitat monetària caigui la capacitat de compra des de gairebé els 51.000 euros fins als 44.800 euros en menys d'una hora, com és el cas del *Bitcoin* durant la matinada del dia divuit d'abril del 2021 representada a la il·lustració 8, una disminució patrimonial en tan sols una hora per un destacable 12.16% sense haver tocat els diners de la cartera, i trobant-se amb la pèrdua de capacitat econòmica de sobte, ja que el gruix de la població no mostra interès per les fluctuacions econòmiques.

A més a més, aquest exemple de volatilitat no és un cas aïllat, ja que com s'observa en el gràfic següent, la volatilitat mitjana a 60 dies del *BTC* respecte al Dòlar durant els dos primers mesos de l'any 2021 supera el 3.5% de variació diària, representant amb la línia negra una xifra molt elevada en comparació amb la volatilitat respecte a l'euro durant el mateix període, en verd al mateix gràfic amb un 0.34%, molt més estable i beneficiós per al sistema financer.

Gráfico cronológico de la volatilidad del Bitcoin



Il·lustració 9. BBWorldWide. 2021. Volatilitat del Bitcoin. Obtingut de <https://www.buyBitcoinworldwide.com/>

Una possible solució per a aquest defecte podria ser l'aplicació de les anomenades *Stable Coins*, un tipus de criptomonedes que compten amb totes les propietats beneficioses que caracteritzen a aquests actius però amb un matís determinant a la seva naturalesa, ja que aquestes monedes electròniques compten amb un factor d'estabilitat total envers al seu preu gràcies a que el valor dels seus *tokens* està directament correlacionat amb un actiu estable.

Aquests factors d'estabilitat poden ser altres criptomonedes o complexos algoritmes que generen la mínima variació possible, tot i que les habitualment es tracta d'una divisa de diners fiat en concret, com podria ser el cas de la criptomoneda *Tether* amb un demostrat èxit al comptar amb una capitalització de mercat propera als \$58 mil milions, una moneda electrònica relacionada amb el dòlar, pel que el seu valor unitari és permanentment d'un dòlar.

Aquesta divisa provoca una millora substancial reduint la mencionada volatilitat cap a un risc molt menor, eliminant el risc de divisa per als països amb el dòlar com a divisa oficial, i minimitzant el risc a mercats com l'uropeu ja que es passa d'una volatilitat extrema del *Bitcoin* cap a la volatilitat controlada del conegut canvi *EUR/USD* entre diners fiat governamentals, fins a cent vegades inferior a la de criptomonedes consolidades com el *Bitcoin*. Al tractar-se d'actius descentralitzats, hi ha moltes alternatives de *Stable Coins* per a dipositar-hi el capital dels inversors, com és el cas del *USD Coin* amb \$14 mil milions de capitalització al mercat, habilitant als inversors un ecosistema monetari on no existeixin les comissions de tercers però on mantinguin la estabilitat del valor del seu capital, en un món encara marcat pel poder adquisitiu en escala de diners fiat, finalment valorant les inversions en euros o dòlars segons el territori, ja que són el medi de canvi establert per a algunes de les compres més importants a les vides de la població com és la compra d'una llar o d'un vehicle, tot i que aquest és un aspecte que podria veure's alterat durant els propers anys.

Per tant, amb l'aparició d'aquestes *Stable Coins* s'aconsegueix eliminar el factor especulatiu i reduir la volatilitat que es relaciona amb el panorama actual de les criptomonedes, tot això sense minvar les excel·lents capacitats com la descentralització i la traçabilitat, entre d'altres, que es mencionen en aquest document. Clarament, és una porta cap al futur transaccional, però el fet de que no serveixi com a font d'ingressos per als especuladors al no canviar mai el seu valor respecte la moneda fiat, genera un ambient sense grans inversors que vulguin popularitzar aquesta alternativa. És una solució excel·lent però una precària font d'ingressos a favor de mantenir el seu valor, pel que caldrà estar atents a aquestes criptomonedes com a opció real de pagaments i transaccions així com a alternativa descentralitzada als dipòsits bancaris tradicionals en un futur proper, al solucionar les principals deficiències de les altres opcions disponibles al mercat.

Un altre inconvenient estructural d'aquest sistema és que, en les criptomonedes amb major reputació com el *Bitcoin* o l'*Ethereum*, aquesta transacció pot arribar a demorar-se durant diversos minuts, un fet que limita completament la capacitat de les principals criptomonedes als negocis físics. Aquesta deficiència d'agilitat transaccional no seria un punt negatiu parlant de transferències bancàries, ja que fins i tot serien més ràpides evitant intermediaris amb rapidesa en poc minuts indiferentment si el destí és nacional o internacional, sense comissions, però sí que suposa un problema en l'àmbit de pagaments immediats.

Tot i així, ja existeixen targetes bancàries amb la capacitat d'emmagatzemar al seu compte una cartera de criptomonedes, i a l'hora de fer el pagament intercanviar-les pels diners fiat de cada territori, sense oblidar que aquest sistema ja implementat per grans empreses com Visa fa esfumar-se les principals característiques d'enregistrament a la cadena de blocs, ja que al cap i a la fi, es tracta d'un pagament tradicional amb prèviament un intercanvi de divises. A més a més, l'acte d'enregistrar una transacció dins de la pròpia *Blockchain*, ja porta associades unes despeses de mineria per a poder apuntar totes les dades en un dels blocs, pagades als usuaris dels nodes encarregats de enregistrar i validar les transaccions sol·licitades segons cada sistema de consens.

Aquests factors poden ser millorats notablement amb l'ús de criptomonedes alternatives amb tecnologies arquitectòniques que han aconseguit una eficiència molt superior al *Bitcoin*, com és el cas de *Ripple* amb transaccions establertes i confirmades en quatre segons de mitjana. De fet, el Banco Santander ja va fer proves durant l'any 2018 amb l'ajuda d'una empresa assessora amb el mateix nom de *Ripple*, degut a que el model de negoci d'aquesta empresa nord americana es basa en l'aplicació a usos reals de la criptomoneda, proporcionant al Banco Santander una gran utilitat lligada a aquesta *altcoin* mitjançant un protocol anomenat XCurrent.

A aquest protocol se li està donant ús integrant-lo en forma de servei per a transferències bancàries internacionals anomenant-lo Santander One Pay FX, posteriorment fent una implementació controlada i monitoritzada, resultant exitosa i donant actualment la possibilitat de transferir divises des de països com Espanya, Regne Unit, Brasil, Polònia o Xile entre d'altres.

Parafrasejant a la presidenta d'aquest banc, la senyora Ana Botín, *“One Pay FX es nuestra apuesta para hacer transferencias internacionales rápidas, sencillas y seguras que aporten valor, transparencia y confianza a los clientes del banco. El Blockchain ofrece grandes oportunidades para mejorar los servicios que damos a nuestros clientes. El lanzamiento de Santander One Pay FX es la primera de muchas funcionalidades que brinda esta tecnología”*.

Clarament, és una innovació destinada a acabar amb els temps d'espera i les grans comissions relacionades amb els girs bancaris internacionals, uns costos gairebé injustificables amb el nivell de globalització actual podent virar cap a una plataforma de pagaments internacionals lligada a contractes intel·ligents encarregats del canvi de divises, generant la possibilitat d'enviar i rebre els diners en efectiu gràcies a la integració de les dades dins de la xarxa de caixers automàtics associats arreu del món.

Aquest suport del Banco Santander és un aspecte clau a tenir en compte ja que, amb el beneplàcit d'una figura tant influent i poderosa com és l'actual presidenta, s'observa clarament com les institucions sistèmiques del món financer ja han avançat des de la fase de resignació enfront a les cadenes de blocs cap a acceptar-les i ser conscients del seu potencial, marcant això un abans i un després cap a la aplicació generalitzada d'aquesta tecnologia emergent.

Paral·lelament, una de les grans innovacions que ens proporcionarà la tecnologia *Blockchain* en un futur proper és el fet de passar dels actuals pagaments programables amb les entitats bancaries cap a un escenari completament nou, un terme conegut en anglès com a *programmable money*, els diners programables.

Aquests darrers, més enllà de permetre establir transaccions monetàries a certes hores concretes com ja es pot fer actualment a la banca tradicional, permetrà la implementació de restriccions tan beneficioses per a la societat com és el fet de bloquejar la compra d'alcohol i tabac als menors d'edat, o també denegant els dipòsits en casos d'apostes tant presencialment com online, reduint notablement un dels problemes emergents actualment a la població envers a les addiccions.

Aplicant una lògica determinada als diners gràcies a la programació dels mateixos, els governs podrien emetre ajudes socials únicament consumibles en bens de primera necessitat, evitant així comportaments potencialment fraudulents respecte a les ajudes socials. Per tant, gràcies a les característiques habilitades per la tecnologia tractada, aquesta nova característica econòmica obrirà tants camins com es puguin imaginar cap a la millora de la gestió monetària del nostre sistema financer ja que aconsegueix definir les propietats associades als diners.

3.7. LES INITIAL COIN OFFERING COM A MÈTODE DE FINANÇAMENT

A la captació de fons mitjançant la *tokenització* se l'anomena *ICO*, l'acrònim del terme anglès *Initial Coin Offering*, considerant-se un dels aspectes més disruptiu de la tecnologia *Blockchain* pel sector empresarial. La seva finalitat és aconseguir diners per a dur a terme projectes professionals, aconseguint-ho mitjançant una oferta inicial de venda de *tokens* virtuals, els quals són allotjats a cadenes de blocs amb la capacitat d'establir *Smart Contracts* automatitzats com és el cas d'*Ethereum*.

Tot i que els *tokens* no comporten un percentatge de propietat sobre el projecte, posteriorment podran utilitzar-se dins del mateix obtenint beneficis com descomptes o capacitat de participació en decisions, encara que habitualment destaca la possibilitat de ser comercialitzats amb el valor que estableixi la llei d'oferta i demanda segons els agents de mercat, obtenint els inversors la diferència econòmica pel canvi de valor directament relacionat amb l'èxit o fracàs del projecte empresarial finançat en cada cas.

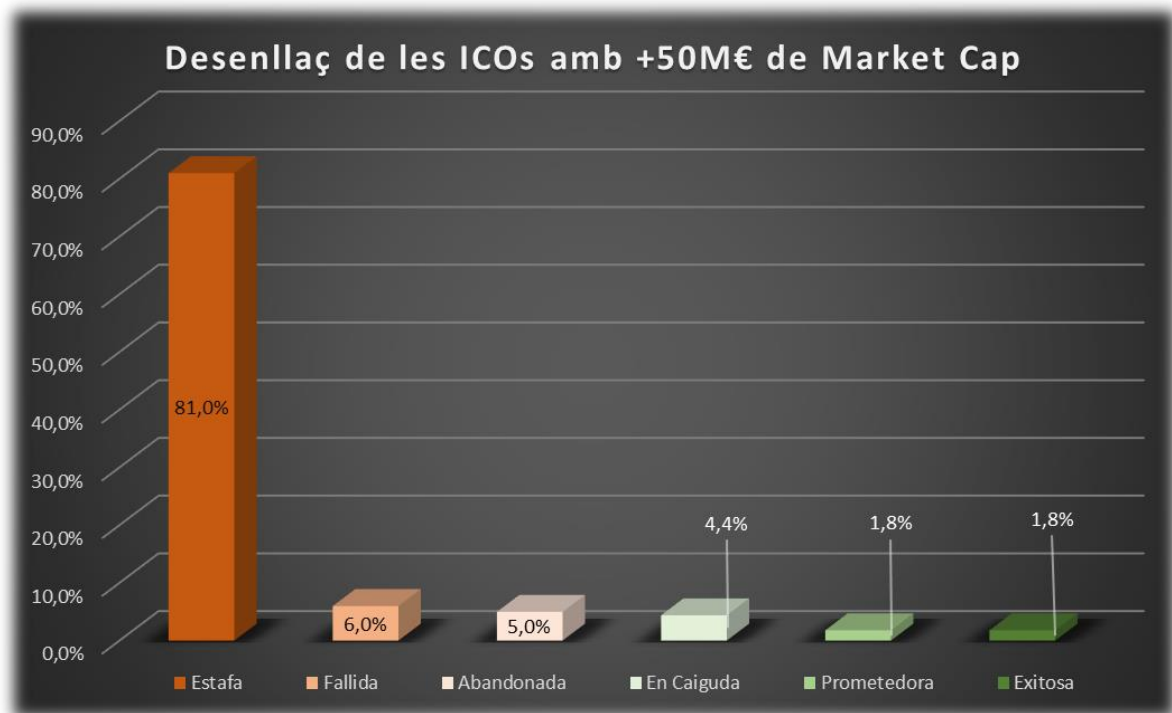
Cal destacar que la característica d'utilitzar els *tokens* com a mètode de captació de fons pot ser un arma de doble fil pels inversors, ja que la gairebé inexistente regulació envers aquest sistema genera molt menys control legal per part de les autoritats competents, podent evitar la presentació de documents que aporten seguretat sobre els projectes finançats mitjançant mètodes tradicionals com les emissions d'accions, proporcionant a les *Initial Coin Offering* o *crowdsales* les condicions idònies per a frauds i estafes empresarials camuflades en una bona campanya de màrqueting inicial, sent una inversió de gran risc i podent arribar a perdre la totalitat del capital aportat pels inversors sense cap defensa establerta de manera concreta al sistema legislatiu actual contra les *ICOs* provadament fraudulentos.

A més a més, en contra d'altres fonts de finançament populars com és el cas del *crowdfunding*, en aquest cas el projecte empresarial no acaba amb la creació d'un producte concret pel mercat generalista, sinó que els recursos seran utilitzats amb lliure criteri empresarial i el valor creat serà canalitzat afectant a la fluctuació de valoració dels *tokens* del projecte.

Un esdeveniment històric que exemplifica aquest risc és la presentació del projecte d'una criptomoneda lligada a l'aplicació de missatgeria Telegram, la *ICO* més gran fins al moment al aconseguir més de mil quatre-cents milions d'euros, però amb tràgic final per als inversors ja que els empresaris encarregats del projecte, després de dos anys, varen decidir no incloure el valor *Gram* al mercat de criptomonedes per problemes legals perdent un judici al Jutjat de Nova York, a causa d'irregularitats als ingressos de l'empresa. Per tant, el fet de no sortir al mercat anul·la qualsevol oportunitat d'obtenir beneficis amb la venda d'uns actius que semblaven molt prometedors per als seus inversors. Cal anar amb especial cura davant aquests projectes, sent conscients que grans beneficis solen ser associats a grans riscos.

Portant-ho a dades reals actualitzades a data del 2018, com indica un estudi de la auditora i consultoria nord-americana especialitzada en actius digitals *Satis Group LLC*, només un 8% de les *Initial Coin Offering* varen portar als seus projectes cap a escenaris exitosos i posteriorment varen poder comercialitzar-se els *tokens* per a que els inversors poguessin obtenir beneficis. D'altra banda, el percentatge de *ICOs* relacionades amb projectes d'estafa o fraudulents s'eleva fins a un destacable 81%, les quals juntament amb projectes abandonats o en fallida augmenten fins al 91% el percentatge d'*Inicial Coin Offerings* que generen pèrdues als inversors, moltes vegades perdent la totalitat dels fons aportats al projecte.

Aquest estudi, amb notorietat de casos reals al ser dut a terme amb *ICOs* que comptaven amb un capital de mercat superior als cinquanta milions d'euros, aporta dades molt impactants alhora que valuoses pels inversors, conscienciant sobre la importància d'estudiar a fons un projecte abans de confiar-hi part del seu capital, veient el precedent històric d'èxit o estafa que destaca el següent gràfic.



Il·lustració 10. Elaboració Pròpia. 2021. Desenllaç de les Initial Coin Offering

És evident que cal que actuïn davant d'aquestes captacions de capital les entitats amb poder legislatiu sobre el sector empresarial, per a la protecció dels inversors envers estafes d'empreses amb projectes fraudulents, preferiblement establint una regularització adient a les característiques de les *Initial Coin Offering* per a poder dur a terme captacions de fons realment beneficioses per la societat com va ser la *ICO* de *Ethereum* durant l'estiu del 2014 recol·lectant més de 15 milions d'euros en un mes i mig, i establint la adequada regulació evitant la prohibició d'aquest sistema emergent de captació de fons com ja ha succeït a països com la República Popular de la Xina, aplicant el seu criteri habitualment tradicionalista en contra de la descentralització.

Per tant, mentrestant no es reguli aquest fet amb defensa pels consumidors davant fets com les estafes i les negligències empresarials dins del sector financer, caldrà que els inversors estiguin minuciosament informats sobre les característiques de cada projecte abans d'invertir-hi, prenent consciència de que el camí a seguir és el de l'adequada regularització d'aquestes captacions de fons per a afavorir el creixement econòmic necessari per al desenvolupament de la població.

3.8. OPTIMITZACIÓ DEL SECTOR PÚBLIC

El potencial assumible dins del sector públic és tan divers com efectiu, eliminant el recorregut altament ineficient que duen a terme la majoria d'administracions públiques al tramitar qualsevol sol·licitud, amb un temps d'espera que s'allarga a diversos dies per fets tan simples com és el registre d'un immoble amb unes dades de propietari o compartir dades entre diverses delegacions i departaments.

El sector educatiu és un dels objectius per a la implementació de les cadenes de blocs per part de grans multinacionals com la nord-americana IBM i la japonesa Sony, unides en aliança per a afavorir la transmissió segura dels registres de dades estudiantils i professionals, un tràmit encara en proves a nivell local però que de ben segur pot canviar el futur de la tramitació relacionada amb l'ensenyament.

Una aplicació molt útil i amb exponencial creixement els pròxims anys és la verificació de documents mitjançant la cadena de blocs, ja aplicada avui en dia en alguns casos concrets de certificacions i títols acadèmics.

Sense anar més lluny, al nostre territori ja hi podem trobar casos reals on la tecnologia de la cadena de blocs s'ha consolidat com a sistema de certificació de diplomes formatius com és el cas de Barcelona Activa, l'agència de l'Ajuntament de Barcelona per al desenvolupament econòmic, la qual mitjançant la validació de competències digitals a través de *Blockchain* permet a les empreses que contractin als candidats sense tenir cap dubte sobre les seves qualificacions, evitant els habituals fraus al currículum a favor d'una total transparència amb la simple implementació d'un codi QR lligat a l'operació que inscriu el contingut del certificat al corresponent bloc de la cadena de blocs, podent consultar-ho en qualsevol moment del futur gràcies a la seva immutabilitat.

Una altra aplicació potencial és l'ús d'aquesta tecnologia com a eina per a dur a terme votacions electorals, tot i que és molt probable que aquest aspecte sigui provat i estès al sector privat amb votacions dins de les pròpies empreses o clubs esportius abans d'arribar al sector públic, com ja s'ha fet a diverses juntes d'accionistes de grans empreses entre elles el mencionat Banco Santander, assegurant-se de que cada persona adequadament identificada amb la seva identitat digital exerceix el seu dret a vot només les vegades que li pertoquin i evitant que aquest vot es vegi modificat de cap manera en un futur. El fet de poder rebre votacions verificades en temps real per a qualsevol consulta, ja sigui vehiculant o simplement a nivell estadístic, augmentaria l'interès per la política que s'està perdent notablement entre les noves generacions degut a una visió generalitzada de no ser components actius del panorama polític tant estatal com autonòmic i local, mantenint un sistema democràtic necessari i essencial per a l'ordre social però recordant que la posició dels polítics és ser representats del poble, pel que caldrà que disposin de totes les tecnologies disponibles per a escoltar als ciutadans.

Aquestes votacions podrien auditar el procediment a temps real, addicionalment podent consultar instantàniament quina és la situació de cadascuna de les persones censades, un aspecte molt explotable estadísticament i que resulta impossible d'obtenir de manera dinàmica amb el sistema de votació actual. A llarg termini podria posar fi a les conspiracions sobre alteracions de resultats electorals, i realment acabar amb la corrupció en països on es cometin aquestes il·legalitats en contra de la democràcia.

També caldrà valorar l'aplicació a la comptabilitat pública per prevenir malversació de fons, una de les principals preocupacions de la ciutadania cap al poder executiu encarregat de gestionar els fons públics. Amb la integració de la *Blockchain* a les administracions públiques, el conjunt de la societat podria arribar a un nivell de confiança cap a l'Estat mai vist fins al moment, per la opacitat del gran camí que recorren els fons públics abans de dona'ls-hi un ús que realment beneficiï a la població.

Aquesta integritat política no es demostra a través de discursos propagandístics, sinó que avui en dia cal que donin un pas endavant i s'adaptin a la transparència que proporciona la cadena de blocs, justificant una administració i gestió apropiades pels fons econòmics que pertanyen al conjunt de la societat.

A més a més, una tecnologia tan potent com aquesta obriria un catàleg d'opcions amb moltes aplicacions a nivell social, com és el cas d'un registre inalterable que reculli els fets delictius i pugui limitar la llibertat de les persones sense la necessitat d'empresonar-les per crims menors i no violents, evitant els costos que això comporta, simplement prohibint els accessos a ubicacions concretes i serveis com el bancari mitjançant les dades lligades a la seva identitat personal.

Aquesta mateixa solució es pot migrar cap a un control d'accés dels menors d'edat a llocs on mai haurien d'accedir però que ho aconsegueixen falsificant certs documents alterables, com és l'ús d'un DNI físic falsificat permetent l'entrada de menors a locals tan populars però tan perillosos com és el cas de les cases d'apostes, reforçant les barreres generades pels diners programables.

La possibilitat de crear una cadena de blocs on poder emmagatzemar informació de manera segura i immutable, genera una possibilitat molt beneficiosa i aprofitable per molts organismes públics, com és el cas dels registres de la propietat o altres tràmits administratius podent dur a terme consultes que per a l'usuari serien amb una interfície molt semblant als actuals núvols d'informació o *clouds*, però evitant l'ús de servidors que podrien ser víctimes d'atacs informàtics com ha ocorregut amb el sistema de dades del Servicio de Empleo Público Estatal, conegut com a *SEPE*, durant el transcurs de la pandèmia sanitària del Coronavirus.

Amb aquest nou sistema als ordinadors de les administracions públiques, es comptarà realment amb una arquitectura informàtica lligada a una seguretat excepcional per a la informació sensible de la població, sense perdre eficiència i facilitat de consulta de les dades necessàries independentment de la Comunitat Autònoma on es consultin, sempre que l'usuari hagi sigut prèviament autoritzat al protocol de seguretat.

En defensa de la transparència amb la que haurien de comptar els polítics de cada país, la tecnologia *Blockchain* genera la possibilitat de dur a terme un seguiment detallat de la distribució dels fons públics recol·lectats amb els impostos aplicats sobre la població, veient realment les seves aplicacions positives per a la societat i evitant un dels grans problemes del sistema polític actual al nostre país, la malversació de fons públics a causa de polítics corruptes.

Amb la implementació d'aquests nous sistemes, l'eficiència del govern augmentaria notablement, pel que la seva adopció en un futur seria clarament positiva. També és aplicable per a combatre els fraus de la població, com és el cas de l'ús inadequat de beques i altres ajudes per part dels contribuents, podent investigar amb quina finalitat han destinat els fons procedents de l'administració de l'estat, la comunitat autònoma o el municipi corresponent.

Per tant, la tecnologia *Blockchain* també serà de molta utilitat a les administracions locals, un organisme on la seva implementació serà molt més senzilla que a les administracions amb competències estatals, generant la possibilitat de no només minimitzar ineficiències greus com la corrupció o els llargs recorreguts de les tramitacions que han de passar per diferents administracions, sinó que també els hi permetrà unificar totes les competències en una mateixa cadena de blocs on allotjar les dades dels ciutadans sense patir per la seguretat ni integritat de les mateixes.

Aquesta seguretat pot marcar la diferència sobretot davant la creixent onada d'atacs informàtics com els *ransomware*, popularitzat per encriptar els documents tant d'empreses privades com públiques durant els darrers anys a canvi d'un rescat econòmic.

En conclusió, encara que inicialment els organismes mostraran certa reticència al canvi i la implementació serà llarga i progressiva, els beneficis d'aquest nou sistema seran notablement positius.

3.9. GESTIÓ DE DADES MODERNITZANT LA COMPTABILITAT

La comptabilitat és un dels departaments amb majors ineficiències a les empreses actualment, ja que tot i disposar d'eines ofimàtiques amb excel·lents capacitats i poder comptar amb *softwares* informàtics d'interfície senzilla específics per a la comptabilització de doble entrada adaptats a cada reglament, les incongruències i disparitats són continues entre empreses, degut tant a errors procedimentals com factors humans.

Aquest és un dels sectors on la tecnologia *Blockchain* podria marcar la diferència durant els pròxims anys, implementant la capacitat de verificar directament des dels nodes de la cadena de blocs inalterable cadascuna de les transaccions comptabilitzades per les empreses.

Algunes contraindicacions d'aquest sistema podrien solucionar-se amb noves alternatives, com seria l'augment de privacitat que es pot obtenir amb les xarxes de consorci o privades que es detallaran més endavant, sempre que es tracti amb informació confidencial. Una vegada siguin superades les adversitats de la implementació d'aquest nou sistema comptable, la seva retroalimentació amb avenços com els *Smart Contracts* podrien arribar a generar un ecosistema comptable amb automatització de les transaccions necessàries, tant sol·licitar el cobrament de factures emeses com l'operació inversa entre moltes altres, juntament amb l'actualització a temps real dels llibres comptables que prenen part a la transacció, facilitant la detecció i prevenció de delictes fiscals així com auditories a qualsevol època de l'any per la facilitat d'obtenir informes de dades, juntament amb una traçabilitat completa per a totes les parts implicades al contracte que els hi permeti tenir plena consciència dels seus moviments comptables.

Amb la possible arribada d'aquesta nova manera de treballar comptablement, els experts han proposat un sistema que promet revolucionar el tradicional sistema de doble entrada, afegint una tercera dimensió als clàssics *debe* i *haber* de les parts implicades a la transacció.

Aquest nou registre s'afegiria a l'actual, comptant amb els registres d'actiu i passiu amb doble entrada gestionat internament per cadascuna de les parts però afegint un registre dins de la cadena de blocs, aplicant a la transacció les característiques d'immutabilitat i seguretat per a una consulta amb confiança per part d'organismes exteriors com auditories o administracions estatals, tenint la seguretat de que aquell registre no s'ha modificat amb cap finalitat de frau fiscal cap altre il·legalitat que es podrien dur a terme amb més facilitat als sistemes actuals de comptabilitat.

En resum, si les organitzacions empresarials i estatals adquireixen la capacitat d'implementar la tecnologia *Blockchain* a la seva comptabilització tant de béns actius com de passius, es deixarien enrere ineficiències sistèmiques com la multitud de desajustos i irregularitats detectades a les auditories anuals que habitualment no són fruit de mala fe, sinó d'un sistema comptable millorable amb la tecnologia actual.

3.10. DIGITALITZACIÓ AL SECTOR FINANCER

La digitalització al sector financer és molt superficial, orientada cap a interfícies modernes desenvolupant aplicacions mòbils i pàgines webs però amb un *back office* molt tradicional i poc actualitzat, sense haver mudat d'arquitectura tecnològica a les últimes dècades, simplement encadenant adaptacions als sistemes informàtics de principis del segle XXI que van salvant el transfons de l'ecosistema informàtic de la banca. Es tracta d'un sector molt competitiu respecte a tecnologies visuals pels usuaris, com és la banca mòbil o la velocitat de les transaccions, però tot el protocol i mecanisme darrera d'aquests procediments ha quedat clarament antiquat amb el pas del temps.

El camí a seguir no passa per continuar aplicant solucions a pedaços, temporals i superficials al sistema actual, sinó que existeix la necessitat d'una reforma integral de la seva arquitectura tecnològica des de l'arrel, per evitar el panorama de ineficiències tècniques amb el que es troben actualment certes entitats bancàries lligades als procediments tradicionals.

Per tant, l'aplicació del *Blockchain* serà extremadament beneficiosa per a aquest sector degut al gran marge de millora i augment d'eficiència amb el que poden comptar, però aquesta tradició conservadora també genera una gran reticència al canvi per part del sector financer. Per a aplicar aquestes novetats disruptives més fàcilment, caldrà veure-ho com una eina de valor favorable a cadascun dels agents del sector, començant pels propis empleats que veuran facilitades les seves responsabilitats diàries.

A més a més, és important tenir en compte que no cal que cadascú entengui al detall el protocol de les xarxes distribuïdes ni tot el transfons de la tecnologia, ja que això augmentaria la dificultat d'adaptació sense aportar grans beneficis.

Simplement, caldrà dirigir una adaptació progressiva tenint present l'objectiu de millora d'eficiència que aquesta nova tecnologia provocarà a cadascun dels agents implicats, orientant-los cap a les conegudes com a *DeFi* pel seu acrònim en anglès de *Decentralized Finances*, mencionades anteriorment.

Aquest protocol financer va més enllà de les ja populars *FinTech*, organitzacions financeres amb base tecnològica per a augmentar la eficiència cada vegada més deteriorada a les entitats financeres tradicionals, a causa de la seva reticència als avenços tecnològics.

Per tant, l'aparició d'aquesta nova arquitectura organitzativa és un progrés que beneficia al conjunt de la societat envers a les possibilitats i capacitats assumibles pel sector financer. Entre les principals novetats que causen aquestes notables diferències, destaca la desintermediació que reduiria les despeses i comissions de gestió cap a tercers al no necessitar la presència de les grans entitats bancàries per a dur a terme qualsevol tràmit, migrant el control del sistema financer per part dels governs estatals i d'aquestes entitats consolidades actualment, cap a la descentralització pròpia dels protocols amb contractes intel·ligents executats automàticament a les cadenes de blocs.

Tot i així, per a materialitzar aquesta exponencial millora d'eficiència, caldrà migrar certs aspectes als quals ja s'ha adaptat la societat cap a d'altres que permetin el sistema de les *DeFi*, com és el cas d'obtenir actius financers mitjançant intercanvis amb entitats emergents com són els *exchanges* de divises, habilitant l'adopció de criptomonedes com el *Bitcoin* o l'*Ethereum* per a dur a terme les transaccions alternativament als diners fiat com els euros o els dòlars.

Són canvis que afecten al capital de la població, un element clarament sensible i que pot generar preocupació al entrar en escenaris desconeguts, però que en un futur es consolidarà ja que els beneficis són molt superior a les possibles reticències al canvi que generarà inicialment, com es pot observar gràficament en el següent quadre.

Propietats	Actualitat	FinTech	DeFi
Nivell d'Eficiència	Poc Eficient	Millora amb la Tecnologia	Molt Eficient
Intermediació	Bancs i Govers	Bancs i Govers	Sistema Descentralitzat
Divisa	Fiat	Fiat	Criptomonedes
Element de Confiança	Intermediaris	Intermediaris	Sense Necessitat de Tercers
Resultat	Tradicional	Transició Tecnològica	Futur

Il·lustració 11. Elaboració Pròpia. 2021. Taula de Diferències entre Tipis d'Entitats Financeres

Dins del propi sector financer, i partint des de la similitud entre la tecnologia *Blockchain* i el registre de transaccions als llibres de comptabilitat, cal destacar que algunes tasques de professionals com els auditors o comptables canviaran dràsticament amb la implementació d'un sistema inalterable i transparent com és la cadena de blocs.

L'evolució dels llocs de treball passa per orientant-se cap a l'anàlisi transaccional des d'un origen, valorant aspectes exclosos de les competències de la cadena de blocs com la legalitat i adequació de les mateixes dins del marc regulador, resolent els conflictes entre parts i auditant la lògica empresarial encara que sigui duta a terme mitjançant els nous protocols comptables.

Això podria portar grans revolucions al sector com el fi de la estacionalitat de les auditories o, com a mínim, una reducció de la càrrega de treball durant els mesos de màxima càrrega de treball, ja que el protocol *Blockchain* permetria auditar la totalitat dels comptes en qualsevol moment que se li programi, així com directament auditant cada transacció al moment d'incloure-la als registres comptables.

Caldrà que els professionals del sector valorin el ventall d'oportunitats que obren les noves tecnologies, evitant la creença popular de que la disrupció tecnològica eliminarà el treball de comptables i auditors, sinó que els obligarà a treballar en un entorn amb noves regulacions i més informatitzat, migrant cap a noves tasques dins de la mateixa professió, obtenint com a resultat un nivell d'eficiència mai vist a la comptabilitat i auditoria empresarial.

Dins del propi sector financer, un dels productes on més comissions s'exigeixen als consumidors són els préstecs bancaris, sobretot en la actualitat quan més enllà dels propis bancs, estan apareixent entitats de crèdit que es basen en microcrèdits qualificables com a abusius pel seu elevadíssim tipus d'interès, beneficiant-se del desconeixement de la població.

Gràcies a la tecnologia *Blockchain*, apareix la possibilitat d'establir un protocol creditici entre els propis usuaris, de consumidor a consumidor, evitant comissions establertes des de una posició de poder.

Així s'aconsegueix un sistema de crèdit basat en les cadenes de blocs, únicament acordant entre usuaris el tipus d'interès que satisfà a ambdues parts, un augment notable d'eficiència que ja el duen a terme sistemes com el *Comerç P2P*.

Aquest terme de *Comerç P2P* és un nom provinent de *Peer to Peer*, dins de la plataforma de Binance, on es troben els usuaris d'igual a igual per a acordar les condicions que estableixen a un *Smart Contract*, i procedeixen a complir-les per el benefici d'ambdues parts.

Aquesta tecnologia obre un ventall enorme d'opcions financeres, com pot ser el cas dels mencionats *Tokens* però amb la finalitat de representar participacions a fons d'inversió, tenint en compte que tot això generarà la necessitat d'adaptar-se a un nou entorn el qual alhora necessitarà noves mesures de seguretat i protecció dels actius financers.

3.11. VALORACIÓ DE L'ELEVAT COST ENERGÈTIC

Com és habitual, tots els aspectes compten amb característiques positives i d'altres negatives, i la tecnologia *Blockchain* no és una excepció. Cal destacar que cap posició extremista sol ser beneficiosa per a la implementació de canvis als sistemes establerts, però les opinions sobre les cadenes de blocs actualment encara són bastant polaritzades.

D'una banda, es troben els fanàtics que ho veuen com a una eina perfecta i sense marge de millora, simplement esperant a la seva implementació complerta mentrestant especulen amb les criptomonedes, perdent-se els aspectes positius d'una acceptació progressiva i orgànica compaginant tecnologies establertes amb les emergents. A la banda oposada, podem trobar els grups d'interès més reticents als canvis, portant a l'extrem un conjunt d'ineficiències que encara presenta la tecnologia *Blockchain* però que són exponencialment millorables en un futur proper, com es detallarà a continuació.

Una de les grans crítiques cap a les criptomonedes és el seu suposat elevadíssim consum energètic, sobretot després de que la gegant multinacional Tesla hagi deixat d'acceptar pagaments amb *Bitcoin* emparant-se en que és un actiu perjudicial per al medi ambient, una afirmació parcialment certa però que necessita molts matisos per a obtenir una visió versemblant de la situació actual.

És objectivament cert que únicament el *Bitcoin* suposa aproximadament el 0.6% del consum mundial total amb gairebé 130 TeraWatts/Hora, unes xifres com les de nacions senceres entre les quals s'inclouen Noruega o Suïssa. Si més no, aquest consum és més de deu vegades inferior al de les entitats bancaries, i quatre vegades inferiors al de la mineria física d'or, aquesta darrera cada vega menys útil per a la societat d'avui en dia.

Sabent aquesta perspectiva, cal recordar que el consum de les cadenes de blocs estarà directament relacionat amb la seva demanda d'ús, pel que si aquesta tecnologia es considerés obsoleta directament el consum d'energia seria mínim, i en sentit oposat, si realment es duen a terme uns consums elevats, és perquè la demanda per a la mineria de nous blocs és també notable i suposaria una millora per a la societat que justificaria el consum energètic.

Aquestes ineficiències ambientals estan directament relacionades amb l'algoritme de consens que s'utilitzi a cada *Blockchain*, consumint molt més els protocols amb *Proof of Work* amb mineria que d'altres com el *Proof of Stake*, ja que no necessita tal consum d'electricitat per a la mineria mitjançant *hardware*, com s'ha detallat anteriorment amb l'arquitectura tecnològica.

Per aquest motiu, lluitant contra una de les seves principals crítiques, diverses criptomonedes estan migrant des dels sistemes de validació *Proof of Work* cap a alternatives més sostenibles com el mencionat *Proof of Stake* que premia la participació amb la possessió dels actius, liderant aquest moviment la segona criptomoneda amb major capitalització de mercat a nivell mundial, l'*Ethereum*, amb el seu llibre de ruta cap a una nova versió 2.0 coneguda com a *Serenity*, millorant tant l'eficiència energètica al deixar de banda la mineria amb *hardware* així com la escalabilitat de la cadena de blocs i la capacitat transaccional de la mateixa, des de la mitja actual limitada a trenta transaccions per segon, molt escassa segons la demanda, cap a un objectiu de fins a cent mil transaccions cada segon.

Per tant, és obvi que la tecnologia *Blockchain* necessita millores i ajustaments per a anar cap a un sistema més eficient, però les característiques de la seva base tecnològica denoten un potencial immens que justifica els esforços per a la millora continua de les cadenes de blocs i els seus protocols.

3.12. TIPUS DE CADENES DE BLOCS PER A CADA FINALITAT

Com s'ha mencionat durant aquest treball, la tecnologia *Blockchain* podria ser definida principalment per tres paraules: redistribució del poder, ja que genera un ambient democràtic de transparència i desintermediació que resten poder a les entitats governamentals i empresarials. Òbviament aquest fet és vist positivament per part de la societat, però compta amb molts detractors, sobretot els propis governs nacionals i grans empreses, perdent privacitat per als seus negocis a favor d'una major exposició social mitjançant les cadenes de blocs públiques.

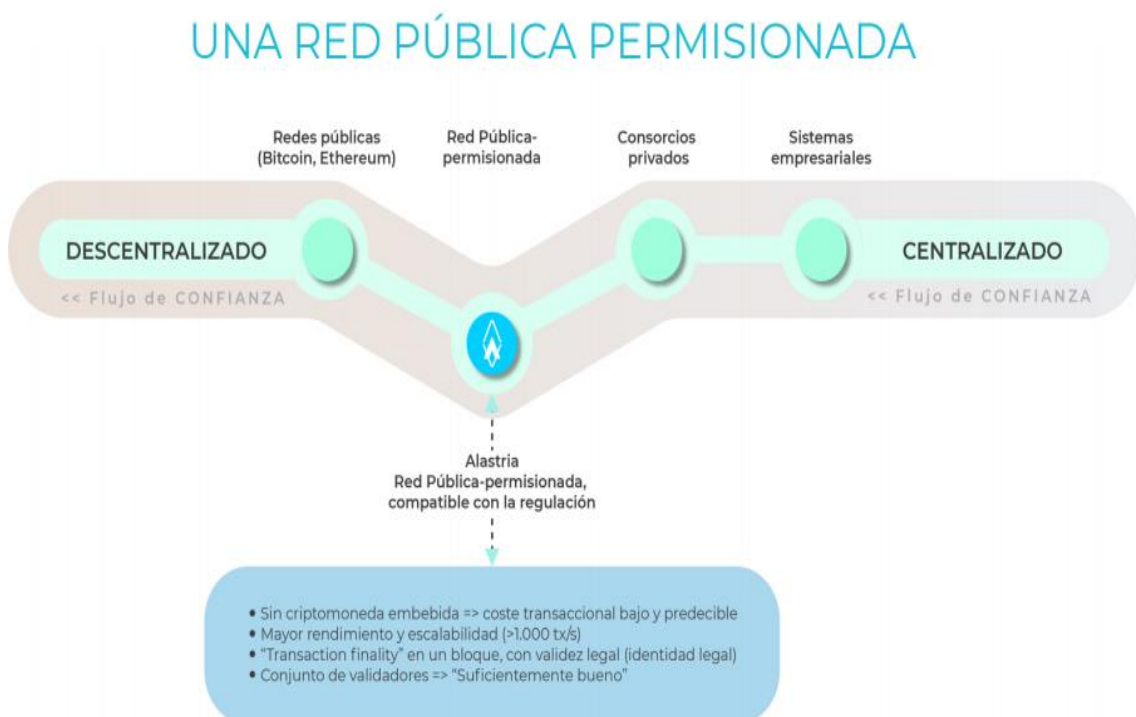
Per aquesta raó, ja han posat en marxa projectes basats en la tecnologia *Blockchain* però amb modificacions que afecten a l'arquitectura de la mateixa, alterant l'essència aportada inicialment per Satoshi Nakamoto.

Aquest és el cas de les xarxes distribuïdes que requereixen necessàriament d'autorització per part dels administradors, tant per modificar la cadena de blocs com per simplement consultar-la, trencant amb l'idea original però aprofitant les grans avantatges d'inviolabilitat sense reduir la privacitat.

Actualment podríem classificar les xarxes *Blockchain* en tres grans categories. La més popular i amb exponencial creixement actualment és la *Blockchain* pública, utilitzada per gegants de les criptomonedes amb xarxes com és el *Bitcoin* i l'*Ethereum*, a les quals es disposa d'accés completament lliure, des de la simple consulta de registres transaccionals fins a la verificació i mineria podent crear nous blocs a la cadena, com s'ha detallat al segon punt d'aquest treball. És a dir, aquest seria un sistema completament descentralitzat i sense cap intermediari amb excés de poder sobre els nodes.

Alternativament, la recerca d'una major privacitat entre parts amb cert poder, ha donat lloc a les mencionades xarxes *Blockchain* de consorci, amb una arquitectura de sistema gairebé idèntica a les públiques però amb canvis que generen una major centralització, podent alterar les autoritzacions de lectura de les dades transaccionals i deixant enrere l'etiqueta de completament descentralitzades, migrant cap a un sistema on els administradors poden establir que la validació dels blocs de la nova xarxa distribuïda sigui responsabilitat de certs nodes del consorci seleccionats explícitament.

Dins d'aquest procediment d'adaptació, cal donar especial notorietat a projectes organitzatius com és el cas de l'organització Alastria al nostre territori nacional, una associació sense cap ànim de lucre i comptant amb la seva pròpia missió per a *"fomentar l'economia digital a través del desenvolupament de tecnologies de registre descentralitzades, la Blockchain"*, una entitat destinada a la col·laboració entre diferents empreses i organitzacions de sectors completament heterogenis contribuint en la creació d'ecosistemes d'innovació.



Il·lustració 12. Alastria. 2021. Diferències des Tipus de Xarxes. Obtinguda de <https://www.alastria.io/>

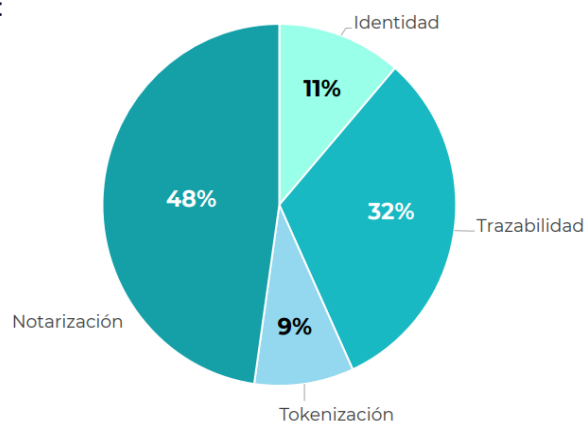
Cal tenir en compte que l'existència d'organitzacions amb poder de grup poden marcar la diferència al comportar un grau superior de confiança, ja sigui mitjançant el cas d'Alastria integrada per les grans companyies nacionals de diferents sectors, com BBVA i Telefónica entre moltes altres, o també mitjançant altres organitzacions més basades a l'àmbit internacional com és la *EEA*, acrònim d'*Enterprise Ethereum Alliance*, formada per multinacionals com J.P.Morgan i Microsoft amb la finalitat de *“permetre adoptar l'ús habitual de Blockchain mitjançant Ethereum a les organitzacions, amb la finalitat de crear noves oportunitats de negoci, aprenent de la mútua col·laboració”*. Per tant, la col·laboració entre entitats davant d'una disrupció de tal importància serà clau per obtenir valor real de l'arquitectura tecnològica mencionada, amb sectors tan diversos com els mostrats en la gràfica següent, on s'observa la distribució dels projectes actuals de la mencionada Associació Alastria.

CASOS DE USO



47 casos de uso desplegados por los socios, con diversidad de aplicaciones:

- Agrifood
- Banca y finanzas
- Legal
- Educación
- Marketing
- ONG
- Participación ciudadana
- Real estate
- Recursos humanos
- Salud
- Turismo
- Transporte y logística
- ...y muchos más



Il·lustració 13. Alastria. 2021. Percentatge Casos d'ús. Obtinguda de <https://www.alastria.io/>

Finalment, cal destacar l'existència de les xarxes *Blockchain* completament privades. Aquestes són creades basant-se en l'arquitectura tecnològica desenvolupada per Satoshi Nakamoto, però deixant de banda els valors socials i de transparència que portava associat el concepte originari, beneficiant-se de la tecnologia de registres distribuïts, en anglès *Distributed Ledger Technology*.

Tot i ser un nou concepte de *Blockchain* que va impactar als precursors de la tecnologia, ja que aquest canvi de propietats deixa de comptar amb la transparència i seguretat que aporten un gran nombre de nodes, la modificació és a favor de la centralització del poder en entitats administradores.

Això no sempre serà beneficiós per a les entitats, podent estancar-se el desenvolupament i millora de les cadenes de blocs per la falta d'incentius cap a la innovació, però així compten amb l'exclusivitat d'escriptura a la seva *Blockchain* privada i poden controlar els usuaris que tinguin dret a veure el seu contingut, necessitant un consum energètic molt menor al ser el consens només entre els nodes privats adjudicats per l'entitat a la seva xarxa de dades distribuïda. És un gran punt de partida per a aquelles entitats reticents a la disrupció tecnològica, entrant progressivament al sistema de la tecnologia *Blockchain*.



Redes públicas

Son redes de Blockchain donde cualquiera en Internet puede participar y ver o validar las transacciones que están teniendo lugar en la red. Ejemplos de redes públicas son Bitcoin o Ethereum



Redes privadas

Son redes con una configuración estática donde un administrador añade los participantes. Suelen ser redes para entornos empresariales y la tecnología más utilizada para crearlas actualmente es Hyperledger.



Redes permisionadas

Normalmente están operadas por consorcios de empresas o instituciones con un objetivo común. Cualquiera puede participar previa aprobación del resto de miembros de la red. Un ejemplo es el consorcio R3 o el español Alastria

Il·lustració 14. Telefónica. 2021. Tipus de Xarxes. Obtinguda de <https://Blockchain.telefonica.com/>

Aquest nou enfocament genera una base de dades en forma de cadena de blocs centralitzada en l'entitat encarregada de la seva creació, molt útil a nivell empresarial tant internament com per a auditories o altres procediments, limitant els nodes de la xarxa o requerint credencials als usuaris, podent treure-hi valor a aquesta tecnologia sense haver de fer públiques dades empresarialment sensibles, variant el protocol d'actuació però mantenint la mateixa estructura de cadena de blocs.

Una característica molt destacable de la *Blockchain* per a les empreses és el seu caràcter permanent, pel que mentrestant segueixi actiu únicament algun dels nodes de la xarxa de dades distribuïda, cada empresa podrà comptar amb un registre inalterable i des dels orígens de tota la seva activitat, acabant amb els immensos arxius físics amb els que compten les grans empreses, a més a més de millorar notablement els temps de recerca de dades dins del propi registre, podent incloure dades sensibles a la competència ja que si s'acullen al desenvolupament privat els hi permet mantenir la confidencialitat empresarial.

Un clar exemple del potencial assumible amb les *Blockchain* privades és el projecte internacional Hyperledger, el qual compta amb la missió de desenvolupar una plataforma inter-empresarial per a la creació de cadenes de blocs centralitzades, basant-se en compartir informació al categoritzar-se com a comunitat *open-source*, comptant amb la col·laboració de les majors multinacionals del món com és el cas de IBM, American Express, Samsung, SAP, Visa o Telefónica entre moltes altres de sectors completament heterogenis.

D'altra banda, cal destacar que aquestes alternatives de *Blockchain* tant públiques com privades no son opcions excloents, ja que poden compenetrar-se perfectament en escenaris concrets.

Un d'aquests escenaris podria ser una major eficiència dins de l'entorn empresarial si utilitzen un protocol de cadena de blocs privada per a la gestió interna de costos i dels temps a la línia de producció, però una altra de pública per a augmentar la transparència i seguretat de les relacions amb proveïdors i clients, beneficiant-se de les característiques de cada una de les opcions que més s'adaptin a les necessitats en cada cas concret.

Cal destacar casos com és el de la República Popular de la Xina, coneguda pel control governamental amb fortes restriccions cap a aspectes que poden alterar el seu poder sobre la seva població com les xarxes socials, un aspecte de control inversament lligat a la descentralització de les criptomonedes i *Blockchain* públiques que afectaria al control del govern de Xi Jinping sobre els seus ciutadans.

Per aquest motiu, el país asiàtic s'ha declarat plenament en contra de les criptomonedes, prohibint tant les seves transaccions institucionals com els conceptes mencionats anteriorment de *Initial Coin Offering* i similars, però posicionant-se plenament a favor de les bases de dades distribuïdes per a aspectes com la identitat digital personal de cadascun dels ciutadans.

Aquesta darrera posició podria semblar contradictòria amb el règim del país, però realment el que no mencionen habitualment és que aquesta base de dades permesa legalment és completament privada, desenvolupada i gestionada pel govern de Xi Jinping, pel que no hi ha res més lluny de la realitat al catalogar el sistema xinès com a tecnologia descentralitzada, sinó que han aconseguit donar un gir de tres-cents seixanta graus a la base tecnològica habilitant un sistema de centralització de dades amb traçabilitat complerta dels seus ciutadans, augmentant encara més el poder del govern.

Aquest és un aspecte a tenir molt en compte de cara a les futures implementacions d'aquesta tecnologia, ja que com es pot demostrar històricament amb invents com l'herbicida conegut com a agent taronja o els explosius per a facilitar la feina als miners, disruptors que teòricament són inofensius i beneficiosos per a la societat s'han de saber gestionar per evitar una reversió dels seus efectes al ser manipulades per les persones inadequades, sent plenament conscients d'aquesta possibilitat.

El poder amb el que compten els governs és clarament un dels punts febles per a l'avenç tecnològic, ja que implantaran barreres legals sense deixar prosperar als projectes que puguin alterar el sistema actual encara que sigui cap a una optimització de la eficiència, situant-se en contra de les tecnologies que els hi causin pèrdues de poder. Per tant, caldrà que la població motivi al govern per a que avanci progressivament cap a un ecosistema eficient i transparent, sense deixar de banda la confiança i simplicitat que s'hauran de lligar a les noves tecnologies per a una millor aprovació de la societat.

3.13. TRAÇABILITAT DETALLADA DELS PRODUCTES

Aquesta és una de les aplicacions més vistoses per al gruix de la societat i amb major implementació ja a la vida quotidiana, podent trobar elements de la tecnologia *Blockchain* a comerços que són visitats a diari com és el cas dels supermercats, ja que la cadena de blocs ens permet comprovar la procedència real dels productes comercialitzat. Aquest és un protocol amb especial interès d'aplicació a productes on la traçabilitat genera valor al consumidor per diferents motius, com pot ser garantir la continuïtat i estabilitat de la cadena de fred als productes congelats, o el fet de la procedència de certs aliments que compten amb diferent qualitat segons el territori d'origen. També és adequat per a finalitats com evitar el frau mitjançant falsificacions i manipulació de les dades d'origen en perjudici dels consumidors, augmentant la confiança entre ambdues parts, i fomentant així el consum responsable en un comerç cada vegada més orientat cap als serveis i la personalització dels productes, aportant un valor necessari per a diferenciar-se de la feroç competència causada per la globalització.

A més a més, també genera un impacte notablement beneficiós per a la salut de la població, tant per al correcte transport de medicaments, com podent fer un seguiment invers dels aliments per arribar a l'origen de possibles infeccions o malalties alimentaries, coneixent cadascun dels procediments i transports als que s'ha sotmès l'aliment ja que solen passar per nombrosos intermediaris els quals aporten el seu valor al producte, podent acotar ràpidament la causa del problema i aplicar les mesures cautelars que es considerin adients a cada situació gràcies a la traçabilitat.

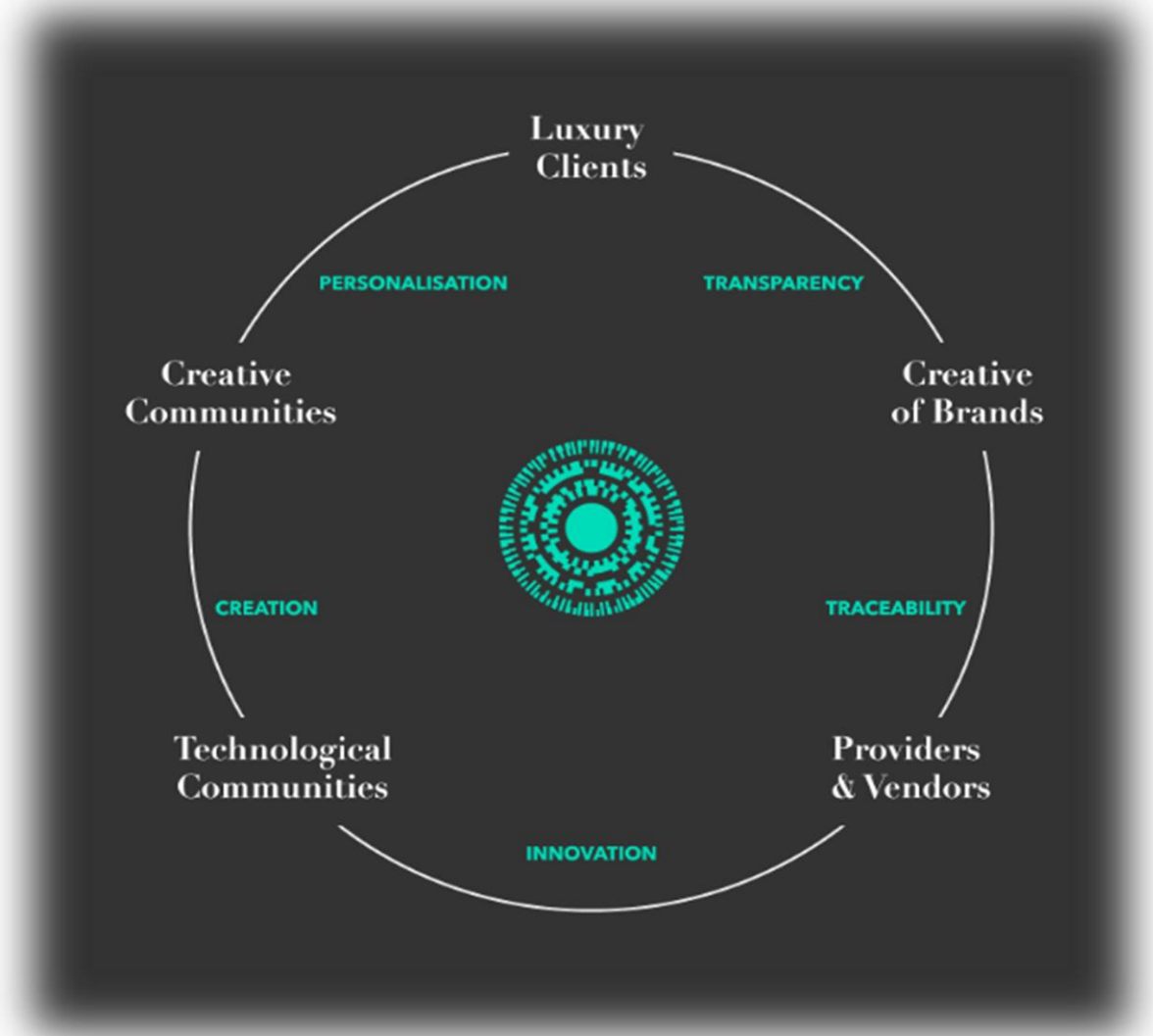
Alternativament, aconsegueix generar molt valor a aquells productes que compten amb antecedents relacionats amb històries d'esclavitud i precarietat, com és el cas dels diamants i altres gemmes luxoses.

En aquest sector de la joieria, poden assegurar als clients una procedència ètica i exclusiva per a les seves joies, evitant pràctiques contraries als drets humans com podria ser l'extracció de diamants mitjançant esclaus i infants, com és el cas dels coneguts com a diamants de sang.

Un exemple clarament beneficiós per a la societat en aquest sentit és Everledger, una organització lligada a la plataforma Hyperledger, amb l'objectiu d'aportar solucions a les joieries de luxe, ja permetent rastrejar milions de diamants des de l'extracció originària del mineral en brut fins a la pròpia boutique de les marques que decideixen comptar amb aquest valor afegit per als seus clients.

Dins del mateix segment del luxe, la majoria de les marques amb més reconeixement a nivell mundial com són les del conglomerat empresarial LVMH, inicials de Louis Vuitton Moët Hennessy, juntament amb altres companyies de la competència com Prada i Cartier així com Bvlgari i Hublot, van arribar a un acord durant l'abril del 2021 per a la fundació del primer consorci de marques de luxe per al desenvolupament de la tecnologia relacionada amb les cadenes de blocs privades, comptant amb el suport de grans empreses del sector tecnològic com Microsoft i ConsenSys, batejant-lo com a *Aura Blockchain Consortium*.

Aquesta entitat, ja activa amb elements de traçabilitat desenvolupats des de la seva base a Ginebra, està orientada cap a la cerca de solucions als problemes de falsificacions que pateixen actualment les marques de luxe, juntament amb el desenvolupament de recursos per a millorar l'eficiència de la seva cadena de subministraments aportant als clients una experiència luxosa més enllà dels materials de qualitat, amb transparència i traçabilitat, deixant les marques a l'alçada del seu renom al adaptar-se als avenços tecnològics tot i ser un sector de confecció tradicional.



Il·lustració 15. Aura Consortium. 2021. Estructura de l'Entitat. Obtinguda de <https://auraluxuryBlockchain.com/>

Al territori nacional també podem trobar-ne exemples que ja són una realitat, com és el cas de l'empresa alimentària Campofrío mitjançant la seva marca de pernils Navidul, permetent la traçabilitat completa dels seus pernils ibèrics, demostrant que el tracte de qualitat cap als aliments del que presumeixen és clarament justificable amb les proves immutables allotjades a la cadena de blocs, seguint els seus pernils des dels camps per on s'alimenten de gla els porcs fins a la venda del producte cap al consumidor.

Un altre exemple dins del propi sector alimentari és el cas de les bodegues de vins, ja que es permet conèixer l'origen i data del raïm així com el procediment i el tracte per part de tots els intermediaris, com recol·lectors o vinicultors, mitjançant BlockWine de l'empresa Amatech, afavorint la defensa de la Denominació d'Origen simplement amb codi QR a l'ampolla que redirigeix qualsevol smartphone a la lectura del bloc de la cadena on s'hi emmagatzema tota la informació, valuosa tant pel productor com pel propi consumidor de l'ampolla de vi. Un exemple d'un altre sistema amb la mateixa finalitat és el que han integrat tant Ernest & Young com EzLab a la cantina italiana Placido Volpone, una bodega vinícola que es diferencia per l'aplicació d'aquesta tecnologia també mitjançant un codi QR, amb venda dels seus productes al nostre país. A la seva pròpia pàgina web donen molta importància a aquest component tecnològic que beneficia a l'experiència dels seus clients, com es pot observar a continuació amb aquesta imatge extreta directament de la pàgina corporativa.

HISTORIA TERRITORIO SELECCIÓN BLOCKCHAIN NOTICIAS TIENDA CONTACTOS

CADENA DE SUMINISTRO CERTIFICADA "VIRTUAL O KM"

Cantina Placido Volpone es la primera bodega del mundo en certificar su cadena de suministro de vino utilizando la tecnología Blockchain. Un libro mayor distribuido que se utiliza para la certificación y la transferencia segura de datos. En la práctica, es una base de datos que contiene un libro mayor de todas las transacciones realizadas entre los usuarios desde su creación, compartido con total transparencia entre los usuarios, sin intermediarios, por lo que cada participante puede verificar la validez de la cadena de transacciones.

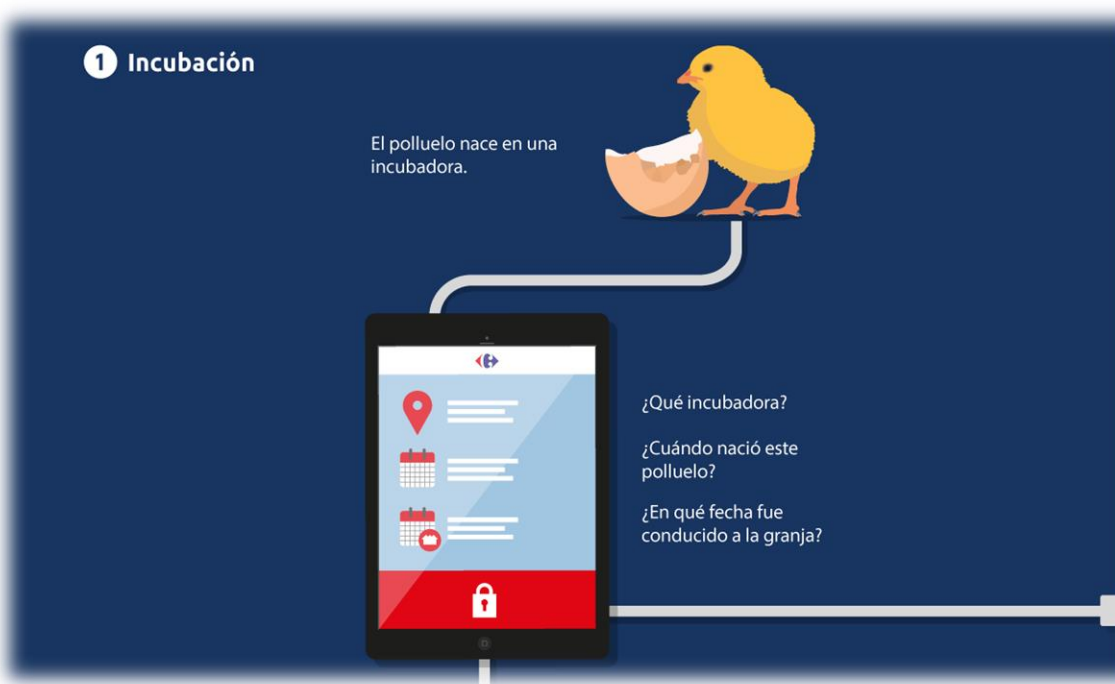
Representa el primer caso en el mundo capaz de autocertificar con total transparencia toda la trazabilidad de la cadena de producción y transformación del vino. Gracias a la solución desarrollada por EY y EzLab, en cualquier momento, el consumidor podrá comprobar el origen, las características organolépticas y toda la cadena agroalimentaria e industrial del vino Plácido Volpone consultando toda la información recogida durante el proceso de elaboración, simplemente acercando su teléfono inteligente al Código QR presente en la etiqueta: desde el campo en el que se cultivó hasta las semillas utilizadas, desde los tratamientos realizados hasta los pasos de la cadena de suministro, incluido el número de "kilómetros" recorridos desde del campo a los estantes de la tienda. Esta es una prueba más de la transparencia que la bodega quiere mantener hacia sus clientes,



Il·lustració 16. Cantina Plácido Volpone. 2021. Aplicació de Blockchain als Vins. Obtinguda de <https://placidovolpone.it/>

A nivell de les grans superfícies, una de les més innovadores amb aquesta tecnologia és la cadena francesa de supermercats Carrefour, mitjançant el seu moviment ecologista *Act for Food* amb el propòsit de mantenir una imatge positiva davant dels seus *stakeholders*, aportant un component de Responsabilitat Social Corporativa molt beneficiós amb el context establert per la societat actual.

Dins d'aquests actes hi destaca principalment la implementació de la tecnologia *Blockchain* als seus productes alimentaris, buscant la traçabilitat acompanyada de transparència i confiança que les cadenes de blocs tenen capacitat d'aportar. Aquest sistema s'està implementant als productes de la marca del supermercat de manera progressiva, amb l'objectiu d'estandarditzar-ho a tots els productes de les famílies Qualitat i Origen a finals de l'any 2022, però funcionant ja actualment en aliments com la llet i el formatge així com els tomàquets i ous de gallines lliures, tot i que va introduir-se a l'any 2018 amb la carn de pollastre ecològic, permetent seguir el procediment del producte com es detalla amb les següents infografies elaborades per la pròpia empresa.



2 Crianza

Son cuatro los intervinientes que introducen sus datos en el portal Internet del blockchain.



El criador indica su nombre y dirección y especifica la fecha en que los polluelos llegaron a su granja y el día de su partida hacia el matadero.



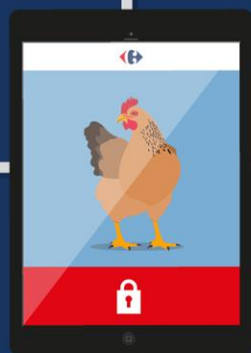
El veterinario oficial certifica que no se ha prescrito ningún antibiótico.



El fabricante de piensos especifica la composición de los lotes suministrados al criador y la ausencia de OGM.



La empresa Certipaq certifica la autenticidad del Distintivo Rojo.

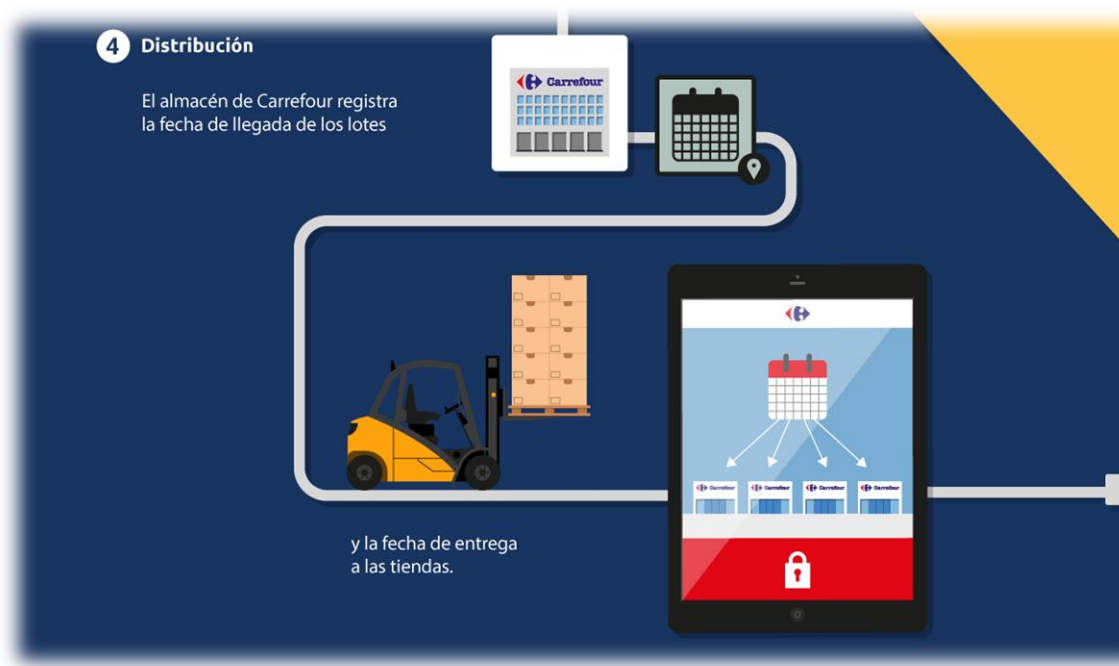


3 Sacrificio y transformación

El matadero, que también se hace cargo del envasado, consigna sus datos de identidad,

el número de lote, la fecha de envío al almacén de Carrefour y la fecha de caducidad del pollo.





Il·lustració 17. Carrefour. 2021. Infografia del Procediment Blockchain. Obtinguda de <https://actforfood.carrefour.es>

Amb aquest protocol de traçabilitat, des de la fase d'incubació dels ous per part de les gallines lliures fins a la distribució per la cadena de supermercats, passant per la cria del pollastre i la seva transformació en aliment envasat i comestible, s'aconsegueix aportar uns components diferenciadors que generen al consumidor una confiança mai vista dins del sector alimentari.

També és una eina útil per evitar les falsificacions, al inscriure a la cadena de blocs aquells productes originals amb una identificació única mitjançant el número de sèrie, com és el cas dels rellotges luxosos, i alternativament també podent evitar la pirateria dels béns amb drets d'autor, com podria ser al món audiovisual permetent comprar i vendre les obres sense la possibilitat de generar còpies falsificades. Alhora, això permet lluitar contra altres crims com és el robatori, sense necessitat de guardar les factures amb el número de sèrie dels nostres béns ja que aquests podrien ser identificats pel propi fabricant i posteriorment seguir amb la traçabilitat de l'objecte, evitant la revenda d'objectes robats al no poder demostrar el seu origen a l'oferir-los a un nou comprador.

Dins d'aquesta aplicació de la cadena de blocs, seran notablement valorades les mencionades *altcoins*, amb procediments de validació diferents al *Proof of Work* de la precursora *Bitcoin*, ja que la limita a unes 6 transaccions per segons generant una latència insuficient dins de grans cadenes de fabricació.

Ja existeixen grans plataformes amb sistemes alternatius, com el *Proof of Stake* de l'empresa dedicada a la traçabilitat VeChain, amb presència destacable a les cadenes de producció de multinacionals com els supermercats Walmart China o la tèxtil H&M, podent validar actualment centenars de transaccions cada segon i amb una projecció cap a les 10.000 transaccions per segon, afirmat per part del seu equip de desenvolupament, amb l'objectiu de superar aquesta xifra que és la capacitat transaccional actual de les grans empreses de pagaments com MasterCard o Visa.

Cal destacar que, una vegada estudiats i desenvolupats correctament, tots aquest avenços a la traçabilitat no només seran beneficiosos per als empresaris experimentant un augment de les seves vendes, sinó que els propis consumidors en sortiran també beneficiats ja sigui mitjançant una major confiança en la qualitat i condició els productes, o amb la reducció de preu associada a la major eficiència a la cadena de producció, entre d'altres beneficis que impulsaran des d'ambdues parts la implantació d'aquesta tecnologia emergent.

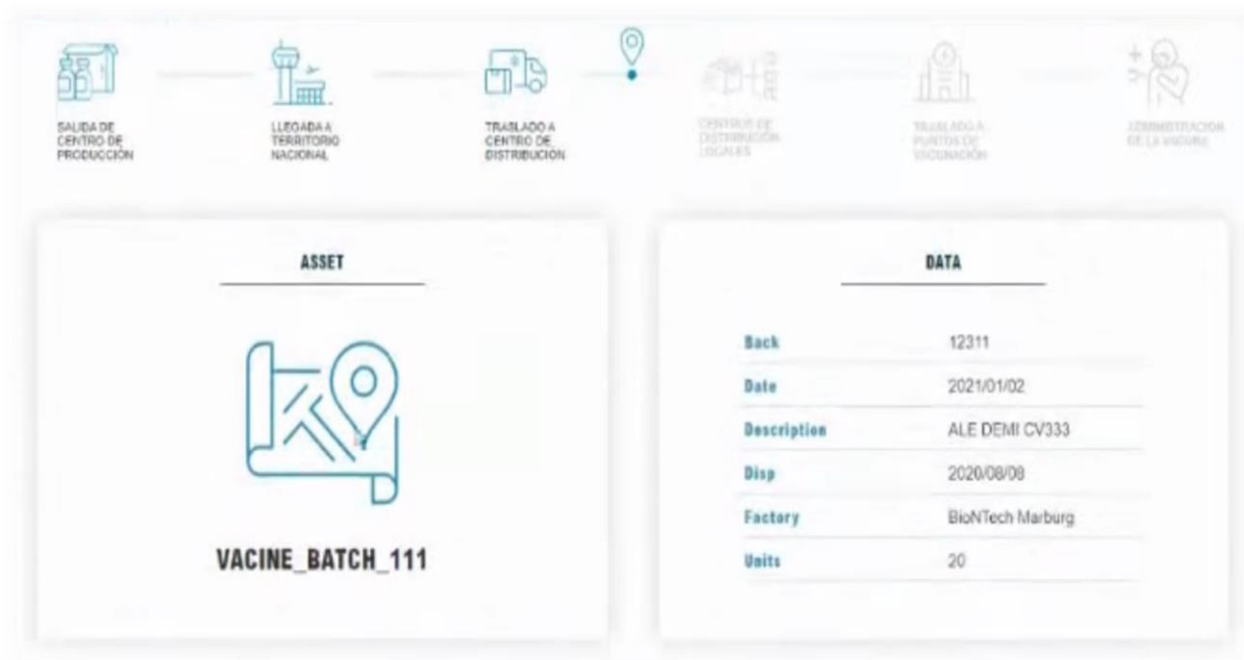
3.13.1. Blockchain Contra la COVID

Finalment, amb la situació inusual viscuda als darrers anys per causa d'una crisi sanitària lligada a l'aparició del virus SARS-CoV-2, conegut popularment com a Coronavirus, la tecnologia *Blockchain* també està tenint un important paper gràcies als beneficis que proporcionen la seva certificació i traçabilitat aplicable a béns tan fonamentals com les vacunes, les quals necessiten que es mantinguin unes condicions estables com la temperatura des del mateix moment de la fabricació fins a la punxada del pacient, movent-se per àmbits internacionals sense cap marge d'error a la seva conservació.

A més a més, lligant tota la cadena de subministrament fins a la punxada final de la vacuna, amb identificació única cap a un pacient en concret, s'obriria la possibilitat de crear un passaport de vacunació amb una font de dades completament fiable.

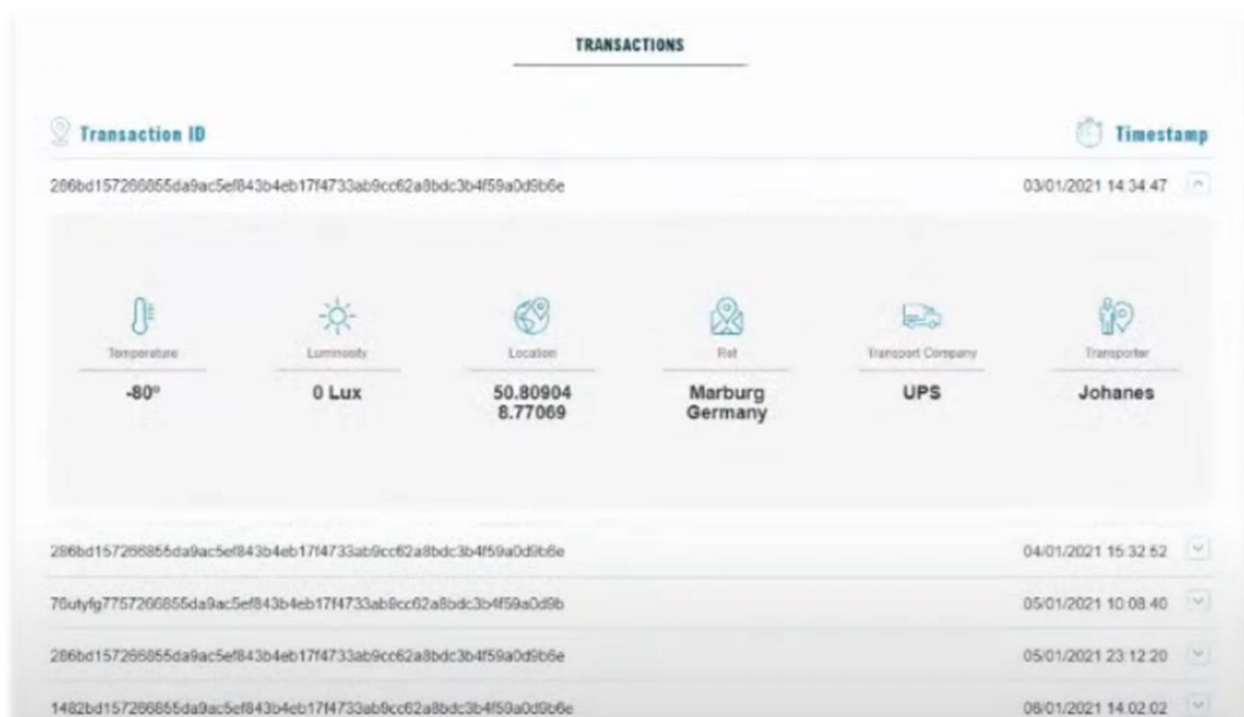
Observant aquest potencial per al conjunt de la població, la multinacional espanyola *Telefónica* ha dut a terme un sistema, mitjançant la seva filial *Telefónica Tech AI of Things*, que ha habilitat el seguiment detallat i minuciós dels enviaments de vacunes cap al nostre país des de la pròpia fàbrica d'origen.

Mitjançant els beneficis de l'arquitectura de les cadenes de blocs detallada a l'inici d'aquest treball, poden obtenir-se les dades expressades a continuació mitjançant una interfície creada per Telefónica, amb l'objectiu de generar una visualització pels seus usuaris de manera clara i concisa.



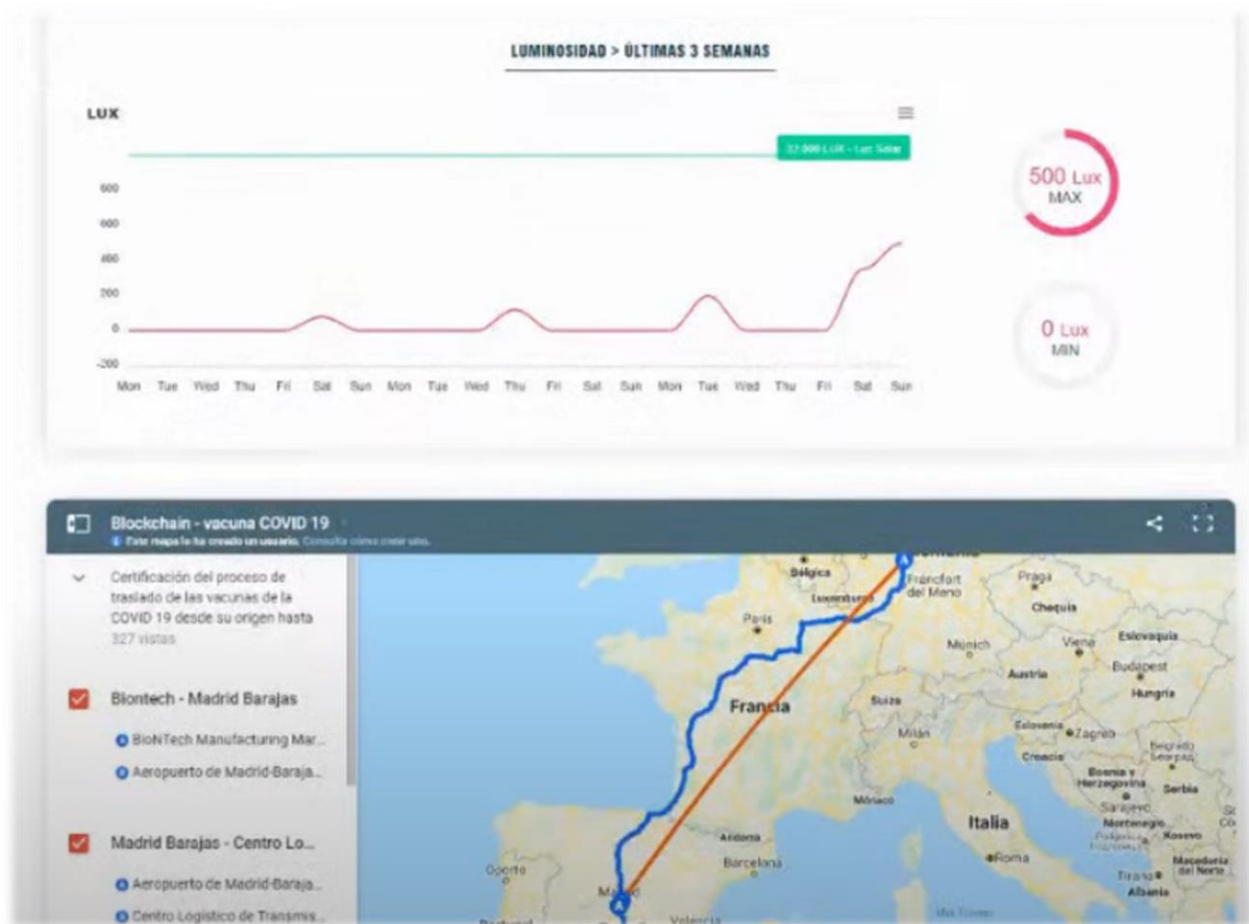
Il·lustració 18. Telefónica. 2021. Interficie de la Traçabilitat. Obtinguda de <https://Blockchain.telefonica.com/>

Com es pot observar, en aquest cas es tractaria d'un enviament de vacunes identificat amb el número de lot 12311, datat a dia dos de gener de l'any 2021, amb 20 unitats procedents de la fàbrica de BioNTech Marburg, actualment havent passat el trasllat al centre de distribució i movent-se cap als centres de distribució locals a Espanya.



Il·lustració 19. Telefónica. 2021. Interficie de la Traçabilitat. Obtinguda de <https://Blockchain.telefonica.com/>

Cadascuna de les transaccions enviades a la cadena de blocs conté unes dades amb dia i hora concrets que poden consultar-se detalladament, com és el cas de la temperatura, la il·luminació a la mercaderia, la localització actual tant en coordenades com en població, i la companyia de transport encarregada de les vacunes així com el conductor concret que està duent a terme el desplaçament.



Il·lustració 20. Telefónica. 2021. Interfície de la Traçabilitat. Obtinguda de <https://Blockchain.telefonica.com/>

Gràcies a les dades mencionades, que són recol·lectades contínuament, s'obté la possibilitat d'obtenir gràfics amb la progressió de cadascuna de les variables, podent controlar que s'hagin complert cadascuna de les condicions necessàries per a preservar el material, habilitant un seguiment gràcies a la tecnologia *Blockchain* amb uns nivells de detall mai vistos fins al moment, sent una clara disrupció per al benefici futur de la població.

3.14. VALOR GENERAT PELS DELS *NON FUNGIBLE TOKENS*

Les àmplies característiques assumibles pels elements de la *Blockchain* provoquen que la innovació no es limiti només a monedes digitals com el *Bitcoin*, estenent les propietats dels elements més enllà de les transaccions econòmiques similars als actuals diners *fiat* imposats per les organitzacions amb poder governamental.

Els anomenats *tokens* es diferencien de les criptomonedes al gaudir de més beneficis favorables als seus propietaris, addicionalment a la funció transaccional com a eina per a dur a terme pagaments, presentant la característica de que mai es consumeixen amb el seu ús, conseqüentment sent també coneguts com a *NFT* per ser les inicials de *Non Fungible Tokens*.

Aquests tenen un gran ventall d'aplicacions, com és el cas de la modernització de les cartes de col·leccionisme que sempre han existit, però afegint-hi un component d'exclusivitat amb el que no compten els cromos tradicionals, ja que en plataformes basades en *Blockchain* com Sorare cadascuna de les cartes dels futbolistes està inscrita a la cadena de blocs d'*Ethereum*, un factor determinant que obrirà una nova alternativa al col·leccionisme físic a favor de la digitalització. A més a més, el valor d'aquests *NFT* és també molt elevat per la seva escassetat, que genera un preu elevat quan compta amb molta demanda i oferta limitada, com es pot observar amb la següent carta única del jugador francès Kilyan Mbappé, venuda per un total de 116,150 unitats d'*Ethereum*, un valor proper als 50.000 euros en el moment de la venda a finals del 2020 però superior als 350.000€ a mitjans de l'any 2021. A més a més, al ser un actiu digital, es duen a terme competicions setmanals segons el rendiment real del jugador amb valors dinàmics associats al *NFT* de la cadena de blocs, una característica mai vista al món del col·leccionisme.

Atributos de carta

Bonificación +51,5%	Nivel 13/20 	XP 7875	Escasez Unique
	Club Paris Saint-Germain FC	Temporada 2020-21	Número de Serie Unique

35097448749899428109200867929277486622796831250893595615442589972105896403753
[Ver la Carta en el Blockchain](#)

Historial de carta

Subasta 29/11/2020

55.105,04 € 116,150 ETH

MaxM

Páginas relacionadas

 Kylian Mbappé Atacante	 Paris Saint-Germain FC Ligue 1
--------------------------------------	--

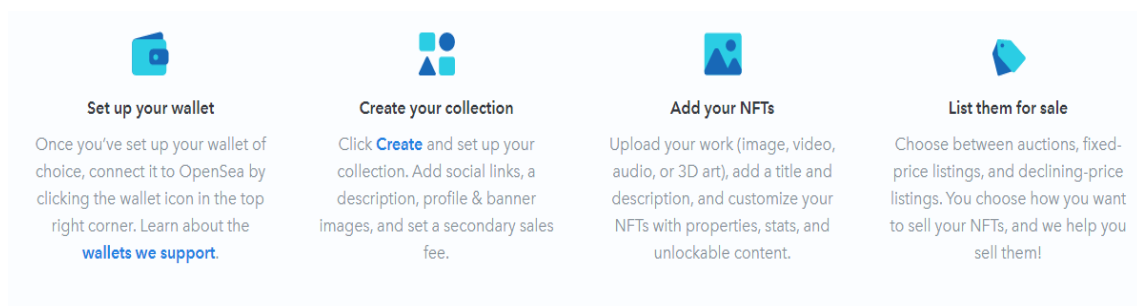
Il·lustració 21. Sorare. 2021. NFT de Kylian Mbappe. Obtinguda de <https://sorare.com/>

Considerant aquests *Non Fungible Tokens* des del punt de vista empresarial, el fet d'emetre *NFTs* genera una oportunitat de recaptar fons econòmics per a nous projectes duent a terme les vistes anteriorment *Initial Coin Offering*, rebent finançament a canvi d'oferir als inversors certs beneficis relacionats amb el projecte finançat, com pot ser el dret a vot durant el desenvolupament del mateix o el dret a comercialització i compra de productes exclusius, entre moltes altres alternatives a disposició de ser establertes per l'empresa emissora segons les característiques de cada projecte.

Per a una millor comprensió del món de possibilitats que obren aquests *tokens*, es durà a terme la creació d'un *Non Fungible Token* propi per a enregistrar el logotip de la criptomoneda creada anteriorment amb finalitat didàctica en aquest mateix treball, anomenada UABCoin.

Amb l'enregistrament del logotip a la cadena de blocs, s'aconseguirà justificar la seva autoria per a la posteritat gràcies a les propietats d'immutabilitat, donant l'opció de vendre aquest actiu digital únic premiant l'esforç dels creadors de contingut, al poder rebre part dels beneficis de les seves obres gràcies a la traçabilitat de les creacions.

Per a la creació dels *NFT* hi ha diverses plataformes amb interfícies preparades per a facilitar el procediment, com és el cas de la que s'utilitzarà a continuació, sent actualment el mercat d'actius digitals més gran del planeta, anomenat *OpenSea*.



Il·lustració 22. OpenSea. 2021. Procediment de Creació NFT. Obtinguda de <https://opensea.io/>

Amb aquesta plataforma, es podran crear Non Fungible *Tokens* de diverses naturaleses, des de música i obres d'art fins a cromos, juntament amb dominis d'internet o vídeos entre molts d'altres. És una alternativa realment prometedora en sectors com l'audiovisual, on els grans segells discogràfics han aconseguit eclipsar els beneficis dels artistes retenint la major part del valor generat mitjançant comissions d'intermediació realment elevades. Convertint una cançó en *token*, l'artista rebria la seva merescuda recompensa en forma de retribució econòmica evitant als intermediaris poderosos.

Posteriorment de la seva creació, tots aquests podran comercialitzar-se per al benefici dels artistes i creadors. Inicialment, caldrà que s'hi adjunti l'arxiu d'imatge del logotip des de l'ordinador propi, anomenant-lo i permetent enllaçar-lo tant amb una pàgina web com amb una breu descripció de l'actiu, com es veu a continuació.

Create new item

Image, Video, Audio, or 3D Model

File types supported: JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF. Max size: 40 MB



Name *

UABCoin

External Link

OpenSea will include a link to this URL on this item's detail page, so that users can click to learn more about it. You are welcome to link to your own webpage with more details.

-

Description

The description will be included on the item's detail page underneath its image. [Markdown](#) syntax is supported.

Logo of the cryptocurrency UABCoin

Posteriorment, les característiques tecnològiques d'aquests *tokens* permeten incloure-hi un elevat grau de personalització, habilitant opcions com el fet d'associar-hi les propietats d'aquell actiu concret, establir barres de nivell segons el progrés associat al *NFT*, mostrar estadístiques de traçabilitat com el nombre de propietaris anteriors, o la redacció de contingut que només podrà veure el comprador de l'actiu, donant-li un punt d'exclusivitat i interès que va més enllà dels aspectes tradicionals de les obres d'art.

Properties

Textual traits that show up as rectangles

+

Levels

Numerical traits that show as a progress bar

+

Stats

Numerical traits that just show as numbers

+

Unlockable Content

Include unlockable content that can only be revealed by the owner of the item.

Explicit & Sensitive Content

Set this item as explicit and sensitive content

Supply

The number of copies that can be minted. No gas cost to you! Quantities above one coming soon.

1

Una vegada decidit el nombre de còpies que vulguin ser creades, en aquest cas una única per a major exclusivitat, es procedirà a la creació del nostre propi *Non Fungible Token*, obtenint com a resultat la fitxa única que s'adjunta a continuació.

Edit

Sell

0

UABCoin

UABCoin

Owned by you

Price History

All Time

No trading data yet

Listings

Offers

No offers yet

Description

Created by you

Logo of the cryptocurrency UABCoin

Com es pot observar, la nostra imatge ja ha obtingut totes les característiques proporcionades per la tecnologia de la cadena de blocs, podent posar-la a la venda i fer un seguiment del seu valor.

Trading History				
Filter				
Event	Price	From	To	Date
Created		NullAddress	you	4 minutes ago

Finalment, es detalla l'adreça del contracte del *Non Fungible Token* a la cadena de blocs escollida, en aquest cas la d'*Ethereum* al ser la més valorada a nivell mundial en relació als *Smart Contracts*, inscrivint-hi la identitat digital única d'aquest *token* que integrarà la imatge de la nostra criptomoneda UABCoin a la cadena d'*Ethereum*, generant un registre de manera segura i inalterable fins a la posteritat.

Details	
Contract Address	0x495f...7b5e
Token ID	7880544956816624...
Blockchain	Ethereum
Metadata	Editable

Il·lustració 23. OpenSea. 2021. Fitxa del NFT Creat a la Blockchain. Obtinguda de <https://opensea.io/>

4. CONCLUSIONS SOBRE EL MÓN D'OPORTUNITATS GENERADES PER LA *BLOCKCHAIN*

Finalment, la posició concloent és que cal tenir en compte a la tecnologia *Blockchain* com als ciments sobre els quals es construirà el futur d'un gran ventall d'aspectes de la societat, com s'ha mencionat detalladament als anteriors apartats. Un protocol sense dies festius ni descansos que encaixa perfectament amb les necessitats de la impacient població actual. Un augment exponencial de proves en registres immutables que apropiaran a la societat cap a un món més just.

Es tracta d'una disrupció tecnològica que canviarà per complert les bases de dades i el *back office* transaccional de les entitats tradicionals, amb una implementació facilitada pel fet de que visualment pot ser molt semblant als ecosistemes amb els que es compta actualment, però obrint un gran ventall de característiques i eficiències sense la necessitat de que els usuaris siguin conscients del funcionament de l'arquitectura tecnològica que hi ha darrera de les interfícies visualment senzilles.

Això és essencial, ja que el conjunt de la societat no té ni les capacitats tècniques per a entendre la complexa arquitectura tecnològica darrera de les cadenes de blocs, ni tampoc cap interès per a aprendre-ho. Per a la aprovació i adopció per part de la població, simplement s'ha d'aconseguir un sistema senzill i efectiu, un objectiu clarament correlacionat amb els valors defensats per la tecnologia *Blockchain*.

Davant de les crítiques a aquesta nova tecnologia disruptiva, cal tenir en compte que no es va passar de la ràdio directament a la televisió d'alta definició, pel que serà completament necessari anar afinant diversos aspectes en un paradigma poblacional que encara no està preparat per a l'arribada d'un canvi amb efectes a tants sectors sense grans canvis als darrers anys, mantenint una inèrcia tradicional que genera comoditat però no comporta eficiència.

Cal tenir en compte que aquest creixement de la tecnologia *Blockchain* s'està produint dins de l'anomenada com a quarta revolució industrial, causada per elements tecnològics com la cadena de blocs i el *Big Data* entre d'altres, com podria ser la interconnexió de maquinaries amb la *Internet of Things* o la digitalització de dades biomèdiques amb beneficis per a la salut.

La disrupció d'aquests elements tecnològics ja és equiparable amb els efectes causats per la màquina de vapor que va provocar la primera revolució industrial a finals del segle XVIII, l'energia elèctrica per a la producció en cadena a la segona revolució industrial des de mitjans del segle XIX fins a la Primera Guerra Mundial, i la darrera revolució industrial al canvi de mil·lenni generada per les novetats electròniques programables i informàtiques. Sense cap mena de dubte, la tecnologia *Blockchain* és una eina per a la transformació del món tal i com el coneixem avui en dia.

Econòmicament, la possibilitat relacionada a la completa desaparició del sistema financer actual és nul·la a curt i mig termini, pel que caldrà mantenir la complementarietat i comparació amb diners *fiat* com l'euro o el dòlar, però sense perdre de vista les solucions financeres aportades per la tecnologia *Blockchain* ja establerta a serveis complementaris al sistema financer tradicional, i avançant a passos gegants cap a una disrupció tecnològica dirigida no tant cap a la substitució de la moneda governamental, sinó clarament cap a una reestructuració sistèmica que pot assolir nivells d'eficiència transaccional i registral impensables temps enrere.

L'elevat component de personalització i adaptació a cadascun dels projectes relacionats amb les cadenes de blocs tant públiques com privades és un element clau per a facilitar la seva implementació, ja duta a terme a sectors tan heterogenis com els que s'han vist durant aquest treball, des del sector bancari fins al tèxtil, des de la creació d'objectes de col·lecció fins al seguiment de vacunes que salvaran vides.

A més a més, és destacable el fet de que els avenços no només seran beneficiosos per a les empreses i inversors, sinó que hi ha un elevat component ètic i social que beneficiarà als països en vies de desenvolupament, obrint portes als menys afavorits per a poder utilitzar sistemes financers dels quals ara se'ls exclou encara que tinguin projectes productius, sent aquesta una tasca humanitària que genera nous escenaris beneficiosos per a totes les parts implicades.

Després de l'anàlisi dut a terme, no queda cap dubte sobre els beneficis que comportarà l'adopció de la tecnologia *Blockchain* en un futur proper, un aspecte disruptiu delicat i que cal seguir desenvolupant però que serà clarament beneficiós per a portar al conjunt de la societat cap a la prosperitat.

La ruta a seguir durant les pròximes dècades no és el negacionisme cap al poder dels governs i altres institucions sistèmiques, ja que un canvi brusc cap a la desintermediació podria crear el caos a la societat actual, sinó que l'extensa adopció progressiva de la tecnologia *Blockchain* tant de manera privada com a organismes públics comportarà implícitament un benefici per a totes les parts de la societat, sense eliminar necessàriament el poder dels organismes escollits democràticament, optant a favor d'una optimització generalitzada que afectarà a tots els segments de la societat.

Amb la realització d'aquest treball de final de grau, s'ha demostrat de manera fidedigna com la tecnologia *Blockchain* és efectivament una excel·lent eina per a la transformació financera. Si més no, el seu potencial d'optimització cap a l'eficiència va molt més enllà, causant una disrupció tecnològica que farà del món un lloc millor.

REFERÈNCIES BIBLIOGRÀFIQUES

ALASTRIA CONSORTIUM. En línia, 2021. Consulta: 20 de maig del 2021. Disponible a l'enllaç: <https://www.alastria.io/>

AMAT, N.; BOAR, A.; PARRONDO, L.; [et al.]; 2018. *Blockchain, Bitcoin y criptomonedas: Bases conceptuales y aplicaciones prácticas*. ACCID Contabilidad y Dirección. ISBN 9788417209728

AMMOUS, S.; 2018. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Published by John Wiley and Sons Incorporation. ISBN 9781119473862

AURA LUXURY. En línia, 2021. Consulta: 18 de maig del 2021. Disponible a l'enllaç: <https://auraluxuryBlockchain.com/>

BANCO SANTANDER ONE PAY FX. En línia, 2020. Disponible a l'enllaç: <https://www.santander.com/es/stories/one-pay-fx-Blockchain-para-agilizar-las-transferencias-internacionales/>

BASHIR, I.; 2020. *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, Smart Contracts, DApps, cryptocurrencies, Ethereum, and more*. Packt. ISBN 9781839213199

BINANCE. En línia, 2021. Consulta: 4 d'abril del 2021. Disponible a l'enllaç:
<https://academy.binance.com/>

BIT2ME ACADEMY. En línia, 2021. Consulta: 1 de febrer del 2021. Disponible a l'enllaç:
<https://academy.bit2me.com/>

BUTERIN, V., 2013. *ETHEREUM WHITE PAPER*. En línia. Disponible a l'enllaç:
<https://Ethereum.org/en/whitepaper/>

CANTINA PLACIDO VOLPONE. En línia, 2021. Disponible a l'enllaç:
<https://placidovolpone.it/>

CARREFOUR *BLOCKCHAIN*. En línia, 2021. Consulta: 1 de març del 2021. Disponible a l'enllaç: <https://actforfood.carrefour.es/Por-que-actuar/Blockchain-alimentario/>

ENTERPRISE *ETHEREUM ALLIANCE*. En línia, 2021. Consulta: 10 de maig del 2021. Disponible a l'enllaç: <https://entethalliance.org/>

ERNEST & YOUNG. En línia, 2018. Disponible a l'enllaç:
https://www.ey.com/es_pa/global-review/2018/restoring-trust-in-the-wine-industry/

ETHIC HUB. En línia, 2021. Consulta: 14 d'abril del 2021. Disponible a l'enllaç:
<https://www.ethichub.com/>

GOLDMAN SACHS; 2016. *Profiles in Innovation: Blockchain, putting theory into practice*. Goldman Sachs Global Investment Research. Disponible a l'enllaç:
https://www.academia.edu/38946070/Goldman_Sachs_Blockchain/

HIGUERAS, J.C.; 2020. *Blockchain, la tecnología disruptiva de la próxima década*. Harvard Deusto, vol. 21. Disponible a l'enllaç:
<https://www.harvard-deusto.com/tag/Blockchain/>

HYPERLEDGER. En línia, 2021. Consulta: 1 de maig del 2021. Disponible a l'enllaç:
<https://www.hyperledger.org/>

INVESTOPEDIA ICO STUDY. En línia, 2018. Disponible a l'enllaç:
<https://www.investopedia.com/news/80-icos-are-scams-report/>

MORGAN STANLEY; 2016. *Blockchain in Banking: disruptive threat or tool?* Morgan Stanley Global Insight. Disponible a l'enllaç:
www.the-Blockchain.com/docs/Morgan-Stanley-Blockchain-report.pdf/

NAKAMOTO, S.; 2008. A peer-to-peer electronic cash system. Disponible a l'enllaç:
<https://Bitcoin.org/Bitcoin.pdf/>

OPENSEA. En línia, 2021. Consulta: 22 de maig del 2021. Disponible a l'enllaç:
<https://opensea.io/>

PLATAFORMA WALLET BUILDERS. En línia, 2021. Consulta: 18 de maig del 2021.
Disponible a l'enllaç: <https://www.walletbuilders.com/>

PREUKSCHAT, A.; 2017. *Blockchain: la revolución industrial de internet*. Deusto Ed.
ISBN 9788498754896

RANKIA CRYPTO. En línia, 2019. Consulta: 10 de maig del 2021. Disponible a l'enllaç:
<https://www.rankia.cl/blog/como-operar-invertir-criptomonedas/>

SORARE NFT. En línia, 2021. Consulta: 18 de març del 2021. Disponible a l'enllaç:
<https://sorare.com/>

TAPSCOTT, A. y TAPSCOTT, D.; 2017. *La revolución Blockchain: Descubre cómo esta nueva tecnología transformará la economía global*. Gestión 2000.
ISBN 9788423426553

TELEFONICA BLOCKCHAIN. En línia, 2021. Consulta: 10 de febrer del 2021. Disponible a
l'enllaç: <https://Blockchain.telefonica.com/>